Worldline ADYTON Cryptographic Module

Hardware Part No: 9071000001
Firmware version: 1.2.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 3

Document Version: 2.0
February 16, 2018

Prepared For:

Worldline SA/NV
Haachtsesteenweg 1442, B-1130
Brussels, Belgium
https://worldline.com/

Prepared By:

EWA-Canada, Ltd.
1223 Michael Street, Suite 200
Ottawa, Ontario
Canada K1J 7T2
www.ewa-canada.com

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose

This non-proprietary Security Policy for the ADYTON hardware cryptographic module by Worldline describes how the ADYTON module meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode.

This document was prepared as part of the Level 3 FIPS 140-2 validation of the module. The following table lists the module's FIPS 140-2 security level for each section.

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

Table 1 - FIPS 140-2 Section Security Levels

1.2 Background

Federal Information Processing Standards Publication (FIPS PUB) 140-2 – *Security Requirements for Cryptographic Modules* details the requirements for cryptographic modules. More information on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP), the FIPS 140-2 validation process, and a list of validated cryptographic modules can be found on the CMVP website:

http://csrc.nist.gov/groups/STM/cmvp/index.html

More information about Worldline, the Worldline ADYTON, and the rest of the Worldline product line can be found on the Worldline website:

https://worldline.com/

1.3 Document Organization

This non-proprietary Security Policy is part of the ADYTON hardware cryptographic module FIPS 140-2 submission package. Other documentation in the submission package includes:

- Product documentation
- Vendor evidence documents
- Finite state model
- Additional supporting documents

The ADYTON hardware cryptographic module is also referred to in this document as the cryptographic module, or the module.

2 Module Overview

Worldline's ADYTON is an innovative high-performance Hardware Security Module (HSM) platform. The design of the ADYTON HSM is based on high security, reliability and robustness, user friendliness, and conformance to international security standards. The ADYTON HSM has an integrated color display, full HEX capacitive keyboard, chip card reader, fingerprint reader, and a USB Host connection.

With its user-centered design, operators are continuously guided through their operations using on-screen wizards. Dual-factor authentication allows for identity-based authentication of operators without keyboard input. The ADYTON HSM can be connected to host systems using its gigabit Ethernet.

The ADYTON HSM can be integrated into an ADYTON HSM rack for installation in standard IT cabinets. ADYTON HSM racks extend the ADYTON HSM with a second gigabit Ethernet interface for network redundancy or separation, and hot swappable dual power supplies for power redundancy.

The ADYTON Cryptographic Module within the ADYTON HSM is a certified FIPS 140-2 module with an overall security level 3. The ADYTON Cryptographic Module detects intrusions, temperature and voltage manipulations, and responds to such attacks by zeroizing its memory where sensitive information is stored by overwriting it.

In addition to its ease of use and high reliability, the ADYTON Cryptographic Module is also designed for performance and achieves thousands of digital signatures per second (benchmarking on 1024 bit). Symmetric key operations can be performed even faster.

With its high security and high reliability, the ADYTON HSM is the ideal product for integration into the complete electronic payment chain (from card personalization, to issuing, to acquiring). But the ADYTON HSM is more than an HSM for financial transactions — it can easily be integrated in other domains where security is becoming more and more demanding such as Public Key Infrastructure (PKI), document signing, E-Health, Smart Metering, chip personalization (e.g. trusted Platform Modules), key generation facilities, and government and military programs.

For more information, please contact:

Filip Demaertelaere, Product Manager
filip.demaertelaere@atos.net

2.1 Cryptographic Module Specification

The cryptographic module is a multi-chip embedded hardware module contained within an ADYTON device. The physical boundary of the module is the tamper detection and response envelope that surrounds the module's components and is then covered in resin. Beyond the cryptographic boundary are the other components that comprise the ADYTON device.

The hardware part number is 9071000001 and the firmware version is 1.2.0.

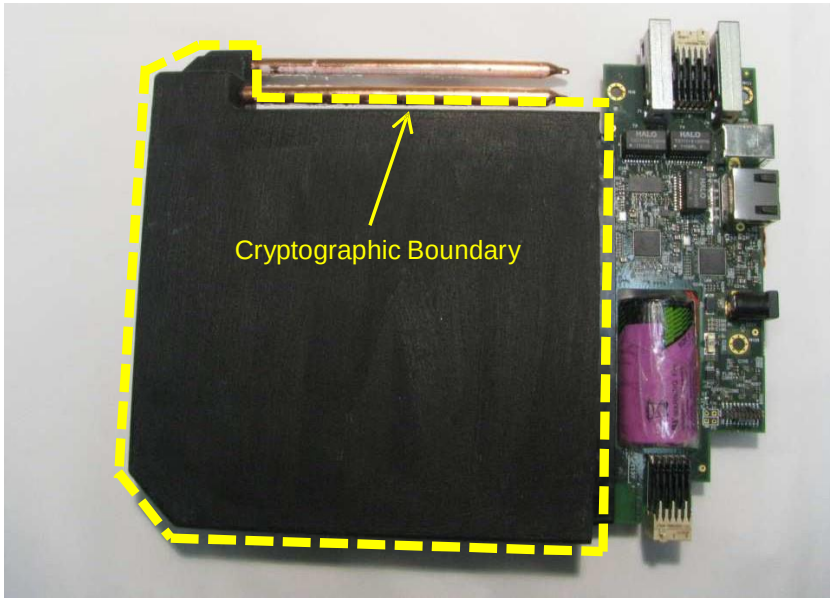

Figure 1 – Worldline ADYTON Cryptographic Module

2.2 Cryptographic Module Ports and Interfaces

The module's ports and interfaces that are supported when operating in FIPS mode are as follows:

2 gigabit Ethernet ports for communication with application hosts (SGMII 1, SGMII 2);
1 USB port called USB Host for a mass storage device to collect the audit trail and to load a firmware image (USB 2);
a UPEK touch fingerprint scanner for operator authentication (USB);
a Smart Card reader for operator authentication (UART1);
a keyboard that uses two physically separated ports, one for password-based operator authentication and manual key component entry (I2C-secure (I2C1)), and the other for control input (I2C-non-secure (I2C0));
a QVGA display (SPI), and LEDs for status output;
a 3.6V battery; and
a 12V power supply.

Table 2 shows how the module's physical interfaces map to the logical interfaces defined in FIPS 140-2.

FIPS 140-2 Interface	Physical Interface
Data Input	Keyboard, UPEK touch fingerprint scanner, Smart Card reader, Ethernet ports, USB Host port
Data Output	Ethernet ports, USB Host port
Control Input	Keyboard
Status Output	QVGA display, LEDs
Power	12V Power Supply, 3.6V battery

Table 2 - Module Interface Mappings

2.3 Roles & Services

2.3.1 Roles

The module uses identity-based authentication and has two operator roles: Crypto Officer and User.

The Crypto Officer role – also known as the Administrator role – is used to manage the module and ADYTON device throughout the lifecycle with the customer. Administrators perform the set-up of the module, select the options and settings for the module, and decommission the module. Administrators are also responsible for managing the Administrator account table.

The User role – also known as the Security Officer role – is used to import key components into the key table. Security Officers are also responsible for managing the Security Officer account table.

The module supports concurrent operators and requires dual-operator control for most Administrator and Security Officer services. Single-operator control services are limited to an operator updating their own account information.

To perform dual-control Administrator services, two or more Administrators must be logged on to the module. The creation of the first two Administrator accounts can be performed freely during initial module configuration without any operator logon. Once two Administrator accounts are in the user account table, additional Administrators can only be enrolled under dual Administrator control.

Dual-control Security Officer services have additional restrictions on the combination of simultaneous Security Officer logons that will satisfy the dual-control requirements. All Security Officer accounts are assigned to one of two Security Officer Groups; Security Officers select whether to enroll to Security Officer Group A or Security Officer Group B during account creation. At least one Security Officer from each Security Officer Group must be logged on to perform dual-control Security Officer services with the exception that two or more Security Officers from Group A can enroll additional Group A Security Officers without requiring the logon of a Security Officer from Group B and two or more Security Officers from Group B can enroll additional Group B Security Officers without requiring the logon of a Security Officer from Group A.

The creation of the first Security Officer Group A and first Security Officer Group B accounts can be performed freely during initial module configuration without any operator logon. Once one Security Officer Group A account and one Security Officer Group B account are in the user account table, additional Security Officers can only be enrolled under dual Security Officer control. When a Security Officer from Group A and a Security Officer from Group B are logged on, all dual control Security Officer services are available. When two or more Security Officers from Group A are logged on (and there is no Security Officer from Group B logged on to satisfy the main dual control requirement), new Security Officers can be enrolled to Group A only. Likewise, two or more Security Officers from Group B can enroll new Security Officers to Group B but not Group A.

2.3.2 Services

The module supports authenticated services as well as services that do not require authentication.

Most authenticated services require the dual control of two authenticated operators. A description of all authenticated services and the operator or combination of operators required to perform the service can be found in Table 3 – Authenticated Services. Dual Administrator services require at least two Administrators to be logged on. Dual Security Officer services require at least one Security Officer from each Security Officer Group (A and B) to be logged on. Owner services are single control services that an authenticated operator (Administrator or Security Officer from either Security Officer Group) can perform on their own account.

A description of all unauthenticated services can be found in Table 4 – Unauthenticated Services.

Service	Operator	Description	Input	Output	Key\CSP
Create Administrator Account	Dual Administrator	Adds a new entry to the Administrator account table that includes user name, role, password, smart card unique identifier, and fingerprint template	Control and Data Input including user name, role, fingerprint, smart card, and password credentials	Status	Operator Password – W Operator Fingerprint Template – W Smart Card Unique Identifier – W
Create Security Officer Group A Account	Dual Security Officer OR At least two Group A Security Officers	Adds a new entry to the Security Officer account table that includes user name, role, password, smart card unique identifier, and fingerprint template	Control and Data Input including user name, Security Officer Group, fingerprint, smart card, and password credentials	Status	Operator Password – W Operator Fingerprint Template – W Smart Card Unique Identifier – W
Create Security Officer Group B Account	Dual Security Officer OR At least two Group B Security Officers	Adds a new entry to the Security Officer account table that includes user name, role, password, smart card unique identifier, and fingerprint template	Control and Data Input including user name, Security Officer Group, fingerprint, smart card, and password credentials	Status	Operator Password – W Operator Fingerprint Template – W Smart Card Unique Identifier – W
Update Account	Account Owner (Administrator or Security Officer)	Updates the password, smart card unique identifier, or fingerprint template of an Administrator or Security Officer account	Control and Data Input via Keyboard command	Status	Operator Password – W Operator Fingerprint Template – W Smart Card Unique Identifier – W
Import Key	Dual Security Officer	Imports a 256-bit AES key into the key table by 2 or 3 key components entered on the keyboard and defines the name of the key	Data Input of key components via keyboard	Status	AES 256-bit Imported Key – W
Decommission	Dual Administrator	Deletes all keys, operator accounts, firmware binary, application binary and license, exports audit trails to a USB device	Control Input via Keyboard command	Status Data Output	All keys and CSPS except Atos Root CA Public Key – Z RSA 4096-bit Atos Root CA Public Key – R RSA 4096-bit Factory Intermediate CA Public Key – R RSA 4096-bit Module Signature Public Key – R
Set Date, Time, Timezone	Dual Administrator	Sets the date, time, timezone	Control Input via Keyboard command	Status	None
Load Firmware	Dual Administrator	Loads firmware update package	Control Input via Keyboard command	Status	None
Self-Test On Demand	Administrator OR Security Officer (from either Group)	Performs all self-tests listed in §2.9.1 Power Up Self Tests	Control Input via Keyboard command	Status	None
Get FIPS 140 Status	Administrator OR Security Officer (from either Group)	Displays FIPS 140-2 status	Control Input via Keyboard command	Status	None

Symmetric Encrypt/Decrypt	Crypto Officer	Firmware low level function used by other services and calling only approved algorithms.	Data, Keys	Status	Symmetric key
Asymmetric Sign/Verify	Crypto Officer	Firmware low level function used by other services and calling only approved algorithms.	Data, Keys	Status	Asymmetric key

R=Read, W=Write, Z=Zeroize

Table 3 - Authenticated Services

The following table lists the supported services that do not require any operator authentication. An authenticated Administrator or Security Officer from either Security Officer Group can also perform these services.

Service	Operator	Description	Input	Output	Key\CSP
Delete Account	Unauthenticated	Removes an Administrator or Security Officer account from the account table	Control Input via Keyboard command	Status	Operator Password – Z Operator Fingerprint Template – Z Smart Card Unique Identifier – Z
Query Accounts	Unauthenticated	Output from account table: username, role, smart card unique identifier, indication if operator is currently logged on and date/time of enrollment	Control Input via Keyboard command	Status	Smart Card Unique Identifier – R
Operator Logoff	Unauthenticated	Displays a list of all logged on operators and allows an operator to explicitly log off 1 or more operators	Control Input via Keyboard command	Status	None
Set IP Configuration	Unauthenticated	Sets the IP configuration	Control Input via Keyboard command	Status	None
Get Serial Number	Unauthenticated	Displays the serial number of the Dallas/Maxim chip	Control Input via Keyboard command	Status	None
Get Name	Unauthenticated	Displays the name of ADYTON device	Control Input via Keyboard command	Status	None
Get Firmware Version	Unauthenticated	Displays the firmware version of the ADYTON device	Control Input via Keyboard command	Status	None
Set Name	Unauthenticated	Sets device name (typically during initialization to identify one ADYTON from a pool of devices)	Control Input via Keyboard command	Status	None
Create Administrator Account (when fewer than 2 Administrator accounts already exist)	Unauthenticated	Adds a new entry to the Administrator account table that includes user name, role, password, smart card identifier, and fingerprint template	Control and Data Input including user name, role, fingerprint, smart card, and password credentials	Status	Operator Password – W Operator Fingerprint Template – W Smart Card Unique Identifier – W
Create Security Officer Group A Account (when no Security Officer Group A accounts already exist)	Unauthenticated	Adds a new entry to the Security Officer account table that includes user name, role, password, smart card identifier, and fingerprint template	Control Input and Data including user name, Security Officer Group, fingerprint, smart card, and password credentials	Status	Operator Password – W Operator Fingerprint Template – W Smart Card Unique Identifier – W
Create Security Officer Group B Account (when no Security Officer Group B accounts already exist)	Unauthenticated	Adds a new entry to the Security Officer account table that includes user name, role, password, smart card identifier, and fingerprint template	Control and Data Input including user name, Security Officer Group, fingerprint, smart card, and password credentials	Status	Operator Password – W Operator Fingerprint Template – W Smart Card Unique Identifier – W

R=Read, W=Write, Z=Zeroize

Table 4 - Unauthenticated Services

2.4 Authentication Mechanisms

The ADYTON employs three different authentication mechanisms: fingerprint authentication, smart card authentication, and password authentication. When a new operator is enrolled, they must register credentials for each form of authentication. Once enrolled, an operator logs on to the ADYTON by entering two of their three credentials. An operator must use either fingerprint or smart card as the first form of authentication entered to log on; the second authentication mechanism can be the password or either the fingerprint or smart card: whichever credential was not used as the first form of authentication.

2.4.1 Fingerprint Authentication

Fingerprint authentication is performed with a fingerprint scanner that complies with FIPS-201. An operator must enroll a fingerprint with the ADYTON; the choice of which finger to use is up to the operator. An operator can change their registered fingerprint template using the Update Account service, but fingerprint templates cannot be deleted as an operator must have credentials for
each form of authentication. The false acceptance rate of the fingerprint sensor is 8.4×10^{-7} (or about 1 in 1,190,476). Assuming that a repeated attack could attempt up to 10 fingerprint entries in a one minute period, the chance that the attack would be successful during a one minute period is 10 in 1,190,476 (or 1 in 119,048) which is less than 1 in 100,000.

2.4.2 Smart Card Authentication

Each smart card has a static digital signature that is generated with the smart card authentication private key over a unique identifier of the smart card; the digital signature and unique identifier are written in the smart card file system during its personalization by the personalization bureau. The smart card authentication RSA key pair is generated by the personalization bureau and the public key is certified by the Atos Technology Provider Intermediate CA; the resulting X.509 certificate is loaded in all smart cards.

An operator is assigned a smart card during enrollment. Once a smart card has been entered in the smart card reader, the ADYTON reads the digital signature, the X.509 certificate, and unique identifier from the smart card and verifies it with the smart card authentication public key. After the card has been verified, the unique identifier is stored in the user account of the operator being enrolled. The ADYTON refuses to enroll with a smart card that has already been linked to an account. An operator can change their smart card identifier using the Update Account service, but the smart card identifier cannot be deleted as an operator must have credentials for each form of authentication.

333

To authenticate using a smart card, an operator enters their smart card into the reader where the ADYTON will read the digital signature, the X.509 certificate, and unique identifier and verify the card with the smart card authentication public key. If the operator's identity is known (i.e. fingerprint authentication has already been performed), the ADYTON will confirm that the unique identifier of the smart card matches that of the operator and log the operator in. If a smart card is entered as the first method of authentication, the ADYTON will search its user accounts for a match with the card's unique identifier and if found, will display the user name.

The RSA 4096-bit Smart Card Authentication Public Key can be considered to have the equivalent bits of security as a 150-bit symmetric key. The chance that a random attempt will be successful is therefore 1 in 2^{150} (or 1 in 1.427×10^{45}) which is less than 1 in 1,000,000. Assuming

that a repeated attack could attempt up to 100 entries in a one minute period, the chance that the attack would be successful during a one minute period is 100 in 2^{150} (or 1 in 1.427 x 10^{43}) which is less than 1 in 100,000.

2.4.3 Password Authentication

Password entry to an ADYTON is performed using a keyboard. An operator can change their password using the Update Account service, but a password cannot be deleted as an operator must have credentials for each form of authentication.

The minimum length for a password is 4 characters. The 133 alphanumeric characters and symbols available for use are listed in Table 5. The chance that a random password attempt will be successful is 1 in 133^4 (or 1 in 312,900,721) which is less than 1 in 1,000,000. Assuming that a repeated password attack could attempt up to 100 password entries in a one minute period, the chance that the attack would be successful during a one minute period is 100 in 133^4 (or 1 in 31,290,72) which is less than 1 in 100,000.

1.,!"#$%&'()*+/:;<=>?@[\]^_`{|}~¡€£¤¥¦§¨©ª«¬-®¯°±²³´µ¶·¸¹º»¼½¾¿Ð×ØÞ ðøþabc2àáâãäåæçdef3èéêëghi4ìíîïjkl5mno6ñòóôõöpqrs7tuv8ùúûüwxyz9ýÿ0

Table 5 - Allowed Characters for Password Use

During password entry, characters are masked by an asterisk.

2.5 Physical Security

The ADYTON is a hardware multi-chip embedded cryptographic module that meets the requirements of FIPS 140-2 Level 4 Physical Security.

The module's tamper detection and response mechanism is provided by an opaque tamper detection envelope that completely encapsulates the module. After the tamper detection envelope is in place around the module, the envelope itself is covered with hard, opaque potting. The envelope detects tamper attempts by penetration (cutting, drilling by conducting or non-conducting drills), removal (unwrapping the envelope, removing the outer coating of the envelope by erosion, milling, or grinding), or chemical attack. The removal of the module's battery or the module's battery voltage going outside the range of 2.5V to 4.4V are also considered to be tamper events and will trigger the module's tamper response.

When tamper detection occurs, the module responds with the immediate zeroization of the Internal Key Wrapping Key (IKWK) that is used to wrap other keys and CSPs stored in non-volatile memory, thus rendering them useless. The module also zeroizes all keys and CSPs stored in volatile memory.

The module protects against unusual environmental conditions or fluctuations that could compromise the module's security. The normal voltage for the module is 12V. The normal operating temperature range for the module is -50°C to 90°C (-58°F to 194°F). If the module detects that the voltage or temperature has fallen outside of its normal operating range, the module responds by zeroizing all plaintext secret and private cryptographic keys and CSPs.

2.6 Operational Environment

The ADYTON uses the QNX operating system to provide a limited operational environment with no underlying general purpose operating system. The FIPS 140-2 requirements for a modifiable operating environment do not apply.

2.7 Cryptographic Key Management

2.7.1 Approved Algorithm Implementations

A list of FIPS-Approved algorithms implemented by the module can be found in Table 6. The module does not implement any Non-Approved algorithms.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
1810	AES	FIPS 197	CBC, ECB, CMAC	128, 192, 256 (bits)	Data encryption Data decryption
138	DRBG	SP 800-90A	Hash SHA-256-based		Deterministic Random Bit Generation
1068	HMAC	FIPS 198-1	HMAC-SHA-256		Message Authentication
2	KBKDF	SP 800-108 KDF	Feedback mode		Key Derivation
907	RSA	ANSI X9.31 key generation PKCS v1.5 and PSS sign/verify		Mod lengths: 2048, 4096 (bits) Public Key values: 65537 (bits)	Key generation Signature Generation Signature Verification
1589	SHA	FIPS 180-4	SHA-256		Message Digest

Table 6 – FIPS-Approved Algorithm Implementations

2.7.2 Non-Approved but Allowed Algorithm Implementations

The module implements a non-Approved but allowed NDRNG which is used once at module power-on to provide input to the Approved RNG. This algorithm is described further in Table 7.

Algorithm	Caveat	Use
NDRNG	NA	Seeding for the DRBG 800-90A.

Table 7 – FIPS-Allowed Algorithm Implementations

2.7.3 Key Management Overview

Key or CSP	Usage	Storage	Generation	Input	Output	Zeroization
AES 256-bit Internal Key Wrapping Key (Master Key) (IKWK)	Used to encrypt/decrypt secret keys and private keys	Volatile memory in plaintext	Internally using Approved DRBG during hardware manufacturing	No	Never	Upon tamper detection or decommissioning
AES 256-bit Internal Key Wrapping Key (Encryption Session Key) (IKWK_ENC_SK)	Used in CBC mode to perform encryption of a key	Volatile Memory	Derived from the AES 256-bit IKWK Master Key using Approved KBKDF	No	Never	Upon tamper detection, decommissioning, or power off
AES 256-bit Internal Key Wrapping Key (MAC Session Key) (IKWK_MAC_SK)	Used in CMAC mode to calculate message digest of a key	Volatile Memory	Derived from the AES 256-bit IKWK Master Key using Approved KBKDF	No	Never	Upon tamper detection, decommissioning, or power off
AES 128-bit Application Encryption Key (Master Key) (AEK)	Used to decrypt Application binaries from Application Provider	NVM encrypted with IKWK, and plaintext in volatile memory during runtime	Outside module	During hardware manufacturing	Never	From NVM at decommissioning or rendered useless by IKWK zeroization at tamper detection From volatile memory upon tamper detection, power off, or decommissioning
AES 128-bit Application Encryption Key (Session Key) (AEK_SK)	Used in CBC mode to perform encryption/decryption of an application binary	Volatile Memory	Derived from the AES 128-bit Application Encryption Key Master Key using Approved KBKDF	No	Never	Upon tamper detection, decommissioning, or power off
AES 128-bit Firmware Encryption Key (Master Key) (FEK)	Used to decrypt firmware and bootloader binaries	NVM encrypted with IKWK, and plaintext in volatile memory during runtime	Outside module	During hardware manufacturing	Never	From NVM at decommissioning or rendered useless by IKWK zeroization at tamper detection From volatile memory upon tamper detection, power off, or decommissioning

Key or CSP	Usage	Storage	Generation	Input	Output	Zeroization
AES 128-bit Firmware Encryption Key (Session Key) (FEK_SK)	Used in CBC mode to perform encryption/decryption of a firmware binary	Volatile Memory	Derived from the AES 128-bit Firmware Encryption Key Master Key using Approved KBKDF	No	Never	Upon tamper detection, decommissioning, or power off
RSA 4096-bit Atos Root CA Public Key	Used to verify certificates	Plaintext in NVM	Outside module	During hardware manufacturing	Yes, at decommission, during export of audit trails	Never
RSA 4096-bit Technology Provider Intermediate CA Public Key	Used to verify certificates	Plaintext in NVM	Outside module	During hardware manufacturing	Never	At decommissioning
RSA 4096-bit Application Provider Intermediate CA Public Key	Used to verify certificates	Plaintext in NVM	Outside module	During hardware manufacturing	Never	At decommissioning
RSA 4096-bit Factory Intermediate CA Public Key	Used to verify certificates	Plaintext in NVM	Outside module	During hardware manufacturing	Yes, at decommission during export of audit trails	At decommissioning
RSA 4096-bit Firmware Authentication Public Key	Used to verify signatures on firmware binaries	Plaintext in NVM	Outside module	During hardware manufacturing or via firmware binary	Never	At decommissioning
RSA 4096-bit Bootloader Authentication Public Key	Used to verify signatures on bootloader binaries	Plaintext in NVM	Outside module	During hardware manufacturing	Never	At decommissioning
RSA 4096-bit Application Authentication Public Key	Used to verify signatures on Application binaries	Plaintext in NVM	Outside module	During hardware manufacturing	Never	At decommissioning
RSA 4096-bit KLD Signature Public Key	Used in challenge/response between ADYTON and KLD during hardware manufacturing	Plaintext in NVM	Outside module	During hardware manufacturing	Never	At decommissioning

Key or CSP	Usage	Storage	Generation	Input	Output	Zeroization
RSA 4096-bit Perso Device Signature Public Key	Used in challenge/response between ADYTON and a Perso Device during hardware manufacturing	Plaintext in NVM	Outside module	During hardware manufacturing	Never	At decommissioning
RSA 4096-bit Smart Card Authentication Public Key	Used to verify signatures on unique smart card identifiers	Plaintext in NVM	Outside module	During hardware manufacturing	Never	At decommissioning
Smart Card Digital Signature	Used during smart card authentication	Plaintext in NVM	Outside module	During authentication process	Never	From volatile memory upon tamper detection, power off, or decommissioning
Smart Card Unique Identifier	Used during smart card authentication	Plaintext in NVM	Outside module	During authentication process	Never	From volatile memory upon tamper detection, power off, or decommissioning
RSA 4096-bit Module Signature Private Key	Used to sign ADYTON internal data	Encrypted in NVM with IKWK, and plaintext in volatile memory during runtime	Internally using Approved DRBG during hardware manufacturing	No	Never	From NVM at decommissioning or rendered useless by IKWK zeroization at tamper detection From volatile memory upon tamper detection, power off, or decommissioning
RSA 4096-bit Module Signature Public Key	Used by external entities to verify signature	Plaintext in NVM	Internally using Approved DRBG during hardware manufacturing	No	Yes, at decommission during export of audit trails	At decommissioning
RSA 4096-bit Module Encryption Private Key	Decrypt Application Encryption Key and Firmware Encryption Key	Encrypted in NVM with IKWK, and plaintext in volatile memory during runtime	Internally using Approved DRBG during hardware manufacturing	No	Never	From NVM at decommissioning or rendered useless by IKWK zeroization at tamper detection From volatile memory upon tamper detection, power off, or decommissioning
RSA 4096-bit Module Encryption Public Key	Used to load the Application Encryption Key and the Firmware Encryption Key	Plaintext in NVM	Internally using Approved DRBG during hardware manufacturing	No	Never	At decommissioning

Key or CSP	Usage	Storage	Generation	Input	Output	Zeroization
SP 800-90 Hash DRBG CSPs (C, V, entropy input, nonce and personalization string)	Used during internal generation of keys	Plaintext in volatile memory	By module's NDRNG	No	Never	Upon tamper detection, decommissioning, or power off
Imported AES 256-bit Key	Optionally entered during the Initial Wizard (initial module configuration at first power-on)	Key component values are XORed before being stored NVM encrypted with IKWK, and plaintext in volatile memory during runtime	Outside module	Manual key entry in 2 or 3 key components via keyboard	Never	From NVM at decommissioning or rendered useless by IKWK zeroization at tamper detection From volatile memory upon tamper detection, power off, or decommissioning
SHA-256 ROM Integrity Test Hash	Used to perform the ROM integrity test at power up	NVM	During hardware manufacturing process	No	Never	At decommissioning
Operator Passwords	Used as one of three methods of operator authentication. Can only be used after fingerprint or smart card authentication has occurred	Protected in NVM with Approved SHA-256 algorithm	Created by account owner	By account owner via keyboard	Never	Overwritten using Update Account service; zeroized at decommissioning
Operator Fingerprint Templates	Used as one of three methods of operator authentication	Plaintext in NVM	Compiled from multiple fingerprint scans by the fingerprint reader for the finger template	By account owner via fingerprint scanner	Never	Overwritten using Update Account service; zeroized at decommissioning
Audit trail log signature	An RSA signature of the Audit trail log generated and output at decommission to a USB token.	No	At decommissioning	No	Yes, at decommission during export of audit trails	At decommissioning

Table 8 - Cryptographic Keys, Key Components, and CSPs

2.7.4 Key Generation & Input

Keys and CSPs that can be input into the module by the customer include:

- Operator Passwords
- Operator Fingerprint Templates
- Imported AES 256-bit Key
- Smart Card Digital Signature
- Smart Card Unique Identifier

Keys that are generated or derived by the module include:

- AES 256-bit Internal Key Wrapping Key (Master Key) (IKWK)
- AES 256-bit Internal Key Wrapping Key (Encryption Session Key) (IKWK_ENC_SK)
- AES 256-bit Internal Key Wrapping Key (MAC Session Key) (IKWK_MAC_SK)
- RSA 4096-bit Module Signature Private Key
- RSA 4096-bit Module Signature Public Key
- RSA 4096-bit Module Encryption Private Key
- RSA 4096-bit Module Encryption Public Key

Operator Passwords and Operator Fingerprint Templates are entered into the module by the operator (account owner) via the keyboard or fingerprint scanner.

The module's Approved RNG (SP 800-90 DRBG) is seeded once with entropy input and a nonce provided by the module's NDRNG at module initialization. The module's DRBG is also seeded with a personalization string that uses the serial number of the module and a value from the real time clock.

The Imported AES 256-bit Key is manually entered in 2 or 3 plaintext key components via the keyboard using the I2C-secure channel.

The module implements SP 800-90A compliant DRBG services for creation of symmetric keys, and for generation of RSA keys as shown in Tables 6 and 8. Resulting symmetric keys are an unmodified output from an Approved DRBG.

2.7.5 Key Output

The following keys are output from the module during decommission:

- RSA 4096-bit Atos Root CA Public Key
- RSA 4096-bit Factory Intermediate CA Public Key
- RSA 4096-bit Module Signature Public Key

No other keys are ever output from the module.

2.7.6 Storage

All Public keys are stored in read/write non-volatile memory (NVM). Secret and Private keys are stored in NVM encrypted with the IKWK, and in plaintext in volatile memory during runtime. The non-volatile memory is erased after tamper detection, power off, or decommissioning.

The Internal Key Wrapping Key is stored in non-imprinting volatile memory and is rapidy erased after tamper detection.

A SHA-256 hash on Operator Passwords is stored in NVM. Operator Fingerprint Templates are stored in plaintext in NVM.

2.7.7 Zeroization

Public Keys are rendered useless when their corresponding Private Key is zeroized. Public keys are zeroized at decommissioning.

The Internal Key Wrapping Key (IKWK) is zeroized upon tamper detection or decommissioning. When the IKWK is zeroized, all keys that were stored encrypted with the IKWK are rendered useless regardless of whether they are zeroized themselves. Secret and Private keys are stored in non-volatile memory encrypted with the IKWK and become useless when the IKWK is zeroized. These keys are also stored in plaintext in volatile memory during runtime and are zeroized in volatile memory upon tamper detection, power off, or decommissioning.

Operator Passwords and Operator Fingerprint Templates can be changed by the account owner using the Update Account service, but cannot be deleted from an account in the user table as an account must always have each of the three forms of authentication credentials (fingerprint, smart card, and password) associated with it. The user account table is zeroized at decommissioning.

2.8 Electromagnetic Interference / Electromagnetic Compatibility

The cryptographic module conforms to the FCC EMI/EMC requirements in 47 Code of Federal Regulation, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

2.9 Self Tests

2.9.1 Power Up Self Tests

The module performs the following tests upon power up and do not require operator input:

Integrity Tests:
- ROM image integrity test using SHA-256
- Bootloader image signature verification using RSA
- Firmware image signature verification using RSA

Self-tests for all validated algorithms:
- AES ECB encrypt/decrypt KATs
- AES CBC encrypt/decrypt KATs
- SHA-256 KAT
- HMAC-SHA-256 KAT
- AES CMAC generate/verify
- RSA ANSI X9.31 key generation
- RSA RSASSA-PKCS#1 v1.5 signature generation/verification
- RSA RSASSA-PSS signature generation/verification
- DRBG SP 800-90 Hash SHA-256 based

Verification that read only partition in non-volatile memory is fused
Atos Root CA self-signed public key certificate verification using RSA
Technology Provider Intermediate CA Public Key Certificate verification using RSA

Bootloader Authentication Public Key Certificate verification using RSA
Firmware Authentication Public Key Certificate verification using RSA
Operator Table integrity verification using SHA-256
Key Table integrity verification using SHA-256
Audit Trail integrity verification using SHA-256

The powers up self-tests are all rerun automatically after every 24 hours of runtime. These self-tests can also be performed on demand by power cycling the module. Each message digest algorithm implements a known answer test separately from any other message digest algorithm.

Failure of the main bootloader authenticity verification will result in the module rebooting continuously. Failure of any other power up self-test will put the module into the Non-Recoverable Error state.

2.9.2 Conditional Self Tests

The module performs the following conditional self-tests:

A pairwise consistency test is performed when an RSA key pair is generated
A digital signature check using the module's Approved RSA algorithm is performed on the loaded firmware when the load firmware service is initiated
A manual key entry test is performed with a key check value when manual entry of key components occurs
A continuous DRBG test is performed whenever the use of a random number is required

Failure of a pairwise consistency test will result in the module rebooting. Failure of the digital signature check will result in the module displaying a message indicating so and refusal to load the firmware. Failure of a manual key entry test will result in the key component not being accepted. Failure of a continuous DRBG test will result in a new random number being generated until the test passes.

2.10 Design Assurance

Configuration management for the module is provided by Concurrent Versions Systems (CVS) which uniquely identifies each configuration item and the version of each configuration item.

Documentation version control is performed manually by updating the document date as well as the major and minor version numbers in order to uniquely identify each version of a document.

2.11 Mitigation of Other Attacks

The module does not claim to mitigate any attacks outside the requirements of FIPS 140-2.

3 Secure Operation

The ADYTON cryptographic module does not support a Non-Approved mode of operation. Upon arrival and first power-up the module is in a FIPS Approved mode of operation and will display "Mode: FIPS" on the General Information screen. No additional configuration is required in order to place the module into a FIPS Approved mode. The FIPS Approved mode status can also be displayed at any time by accessing the General Information screen through the main menu.

3.1 Initial Key Loading & Personalization

The module arrives to the Application Provider in a FIPS Approved mode of operation. This section provides additional background information about the initial key loading and personalization of the module that occurs at the manufacturing facility, the Atos Key Management Facility, and the Application Provider Key Management Facility, all before the module is delivered to the customer.

Many of the module's keys are generated and loaded onto the module by the manufacturer before the module is delivered to the customer. Key generation and input that occurs after the module is delivered to the customer is discussed in section 2.7.3.

The initial key loading process takes place at the manufacturing facility in a secure room with operational procedures that guarantee the module's authenticity. A separate module connected to a PC acts as a Key Loading Device (KLD) to commission modules for customer use. The KLD performs the loading of keys onto the module via the module's Ethernet port.

The following steps are performed during initial key loading:

generate Internal Key Wrapping Key
generate and certify Module Signature Key Pair
generate and certify Module Encryption Key Pair
write Factory Intermediate CA Public Key
write Application Provider Intermediate CA Public Key
write Application Encryption key
write Firmware Encryption key

The Internal Key Wrapping Key, Module Signature Private and Public Keys, and Module Encryption Private and Public Keys are all generated internally using the FIPS-Approved DRBG.

The Atos Root CA Key Pair is generated in the Atos Key Management Facility. The public key is loaded in ROM during the manufacturing of the module. The private key is never loaded into the module and does not leave the Key Management Facility.

The Firmware Authentication Key Pair, Bootloader Authentication Key Pair, and Technology Provider Intermediate CA Key Pair are also generated in the Atos Key Management Facility. The Application Authentication Key Pair is generated in the Application Provider Key Management Facility. The Bootloader Authentication Public Key and Technology Provider Intermediate CA Public Key are included in the bootloader binary, and the Firmware Authentication Public Key and Application Authentication Public Key are included in the firmware binary and application binary, respectively, and they are all loaded in the module when the binaries are installed. The private keys are never loaded into the module and do not leave the Key Management Facility.

One instance of the KLD Signature Key Pair and Perso Device Signature Key Pair are generated for each Key Loading Device and Perso Device instance. The manufacturer operates the Key Loading Devices and generates the KLD Signature Key Pair. An Application Provider operates the Perso Devices and generates the Perso Device Signature Key Pair. The KLD Signature Private Key and Perso Device Private Key are never loaded into the module.

3.2 Administrator Guidance

Administrators manage the module and ADYTON device throughout the lifecycle with the customer. Administrators perform the initialization of the module, select the options and settings for the module, enroll other Administrator accounts, load firmware and application software, and decommission the module.

All logged on Administrators are responsible to check the actions that are triggered on the module.

3.3 Security Officer Guidance

Security Officers enroll other Security Officer accounts and perform tasks with the keys in the key table including the importing of key components.

All logged on Security Officers are responsible to check the actions that are triggered on the module.

4 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CVS	Concurrent Versions System
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
EFP	Environmental Failure Protection
EMI/EMC	Electromagnetic Interference / Electromagnetic Compatibility
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
HMAC	(Keyed-) Hash Message Authentication Code
IKWK	Internal Key Wrapping Key
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
KLD	Key Loading Device
KMF	Key Management Facility
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
NDRNG	Non-Deterministic Random Number Generator
NVM	Non-Volatile Memory
QNX	QUNIX or Quick UNIX
QVGA	Quarter Video Graphics Array
ROM	Read Only Memory
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
TDES	Triple Data Encryption Standard
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus

Table 9 - Acronym Definitions