CHR CRYPTOGRAPHIC MODULE - FIPS 140-2 NON-PROPRIETARY SECURITY POLICY

DOCUMENT NUMBER	:	CHR/LP51028/EN
VERSION	:	1.3
DOCUMENT DATE	:	06 May 2022
NUMBER OF PAGES	:	17

version: 1.3 **document number:** CHR/LP51028/EN

CHR Hardware version 006/D & 006/E
Firmware version V1.06-03L

Disclaimer:

Atos
Rue Jean Jaurès
BP 68
F-78340 LES CLAYES SOUS BOIS
Phone: + 33 1 46 25 54 58

Contents

List of figures

List of tables

1 Introduction

The CHR Cryptographic Module (CHR) is a multi-chip standalone module providing functionality for the secure loading of applications, and ensuring the integrity of any loaded application. The application shall previously be signed using the private key of a Certification Authority (CA).

The secure loading includes verifying the signature of the application. This is achieved by the Loader executing the following steps:

- Opening the Application Provider Public Key Certificate,
- Verifying the Application Provider Public Key Certificate using the CA Public Key,
- Computing the Application hash,
- Verifying the hash signature using the Application Provider Public Key.

This mechanism ensures that only applications signed by the Application Provider can be loaded in the CHR.

Only FIPS-Approved algorithms are implemented in the CHR for signature verification. As a consequence, the CHR only supports the Approved mode of operation.

The validation is only for the CHR. It does not include the loaded applications.

1.1 Objective of the Document

The CHR Security Policy document is intended to be part of the CHR FIPS documentation.

The document relates to CHR Cryptographic Module versions 006/D and 006/E.

The objective of the document is to define the CHR Security Policy. The document details the security rules under which the CHR cryptographic module operates. Rules include those required by FIPS and additional CHR module rules.

This document is structured as follows:

- The current section is an overview the CHR cryptographic module.
- Section 2 defines the Identification and Authentication Policy
- Section 3 describes the Access Control Policy
- Section 4 specifies the Physical Security Policy
- Section 5 addresses the Self-tests
- Section 6 defines Security Officer and User guidance.

1.2 CHR Overview

Additional information regarding the physical security mechanisms is provided in section 4.1.

The CHR includes hardware and software components.

The hardware component stores software code and processes sensitive data. These storage areas described will be zeroized in the event that the metal cover is breached, due to internal zeroization circuitry. The hardware component includes two secured memory areas respectively named “sec-memory A” and “sec-memory B”. Secured memory is used to manage sensitive data (e.g. keys).

The hardware component also includes a flash memory divided into two partitions (“partition-A” and “partition-B”). A loaded application may reside in and be executed from either “partition-A” or “partition-B” depending on the Application Provider’s requirements.

The software component is the Bootstrap/Loader. The software component is securely stored in the hardware component.

The Bootstrap part of the Bootstrap/Loader provides services such as system initialization including reset, auto-tests, and conditional tests.

Following the execution of the initialization and auto-tests by the Bootstrap, and based on a request from the serial port, the control is transferred to the Loader. If no request is received from the serial port then the Bootstrap transfers the control to the Application. The control is given to Application either in "partition-A" or "partition-B" depending on a toggle under the control of the Application Provider. The management of the application toggle is outside of the scope of this document.

The Loader is designed to securely load applications. Loading an application is achieved through the serial port. As a first step the Loader erases secured memory areas ("sec-memory A" and "sec-memory B"). Then the Loader securely loads the Application. Conditional software load tests apply during the loading of the application.

The secure load process includes signatures verification. The Loader computes a hash using SHA-256 according to FIPS 180-4. The hash function is used by the RSA signature verification algorithm according to RSASSA-PKCS1-v1_5. The Loader verifies the Application Provider's public key using the CA Public Key stored in the CHR. The Loader then verifies the application's signature using the Application Provider's public key. Authentication methods are detailed in section 2.1.

After successful signatures verification the Loader registers the Application in "partition-A" and transfers the control to the Application.

Loaded Applications intended to execute with this module are not included as part of this validation. Once control passes from the Loader to the application (an application has been started), this validation doesn't apply any more. Any future validation scenario, whereby an application is included as part of the cryptographic boundary, will be validated separately from this validation.

The following interfaces are supported by the CHR:

Logical Interface	Physical Interface
Data Input interface	Serial Port
Data Output interface	
Control Input interface	Serial Port, power button
Status Output interface	Serial Port, power LED, Front panel display
Power Interface	Two hot plug 100/240 VAC Power Interfaces

Table 1 CHR Interfaces

Three cards manage the interfaces.

The Power Interface is connected to the power source used to maintain the non-volatile memory.

The Power Interface is under the control of the CHR.

The Status Output Interfaces are power LED and a two-line display used to indicate the status of operations. Status output can be seen from the serial connection as well. The LED and display are under the control of the Bootstrap/Loader.

The Data Input Interface is provided by the asynchronous serial port under the control of the Bootstrap/Loader. Although the Application(s) controlling the Ethernet ports are not within the scope of this validation, the Ethernet ports are capable of data input/output when controlled by an Application. Data input is also provided by the console connection over which applications are loaded.

1.3 CHR Product Family

Figure 1 CHR Front Panel Picture

The CHR is the corner stone of a range of security products developed and signed by Atos as Application Provider. Additional products may be developed by Application Providers, based on the CHR.

As stated above, Applications developed by Application Providers and intended to execute with CHR module are not included as part of this validation.

1.4 Targeted Security Level

The CHR cryptographic module including the Bootstrap/Loader is targeted to fulfil the following security level according to the FIPS Security Requirements

FIPS 140-2 Section	Target Level
Cryptographic Module Specification	3
Cryptographic Module Ports & Interfaces	3
Roles, Services, & Authentication	3
Finite State Model	3
Physical Security	3 +EFP/EFT
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall Level	3

Table 2 FIPS140-2 Target level

2 Identification and Authentication Policy

This section specifies the identification and authentication policy for CHR. The roles and their associated authentication methods are listed.

2.1 Roles and Authentication Mechanisms

The CHR supports an authentication mechanism relying on RSA signature verification. This authentication mechanism applies for secure loading and secure starting of an application. Four components are involved in this authentication mechanism, the CA private key, the CA public key, the Application Provider (AP) public key, and the signature of the Application.

Role	Type of Authentication	Authentication Data
User	Identity Based	2048 Bit RSA Public Key (AP)
Security Officer "Crypto Officer"	Identity Based	2048 Bit RSA Public Key (CA)

Table 3 Roles & Authentication Data

An Application Provider (User) is authenticated with an RSA 2048 bit public key (AP) before the provided application is started. If the signature can be validated, the application can be started by the module.

New applications may be generated and signed by the Application Provider using the AP private key that is held securely by Application Provider.

Authentication of the Security Officer is provided by secure manufacturing procedures at the factory.

The Security Officer role involves the loading of a 2048 bit public key (CA) into the module at the factory. The CA public key is used by the module to verify the signature chain on any application that it loads. An authorized Security Officer performs the loading of the CA public key at the factory. Once the module is fielded, the Application Provider public key may be signed by the Security Officer using the CA private key that is held securely at the factory. (Security at the factory is provided by procedural controls.) In the field the Security Officer, acting on behalf of the factory, may load the signed AP public key along with the signed application into the module where the signatures are verified using the public keys. This is the only cryptographic application offered by the module's software.

2.2 FIPS Approved Mode of Operation

The CHR only supports the Approved Mode of Operation. The Approved Security Methods defined in section 2.3 shall be used to support the FIPS Approved Mode of Operation.

When the self-test report has been printed on the status output interface (serial port), as shown in section 5.1, the display is green as mentioned in Table 9 (application running) when self-tests have successfully completed, thus the module is operating in the Approved mode.

2.3 FIPS Approved Security Methods

The module keys map to the following algorithms certificates:

Approved Security Function	Certificate
Signature verification 2048 bits	
RSA • **PKCS#1 (FIPS 186-4)**	Certificate #A935
SHS-256	
SHA-2 byte-oriented (FIPS 180-4)	Certificate #A935

Table 4 Approved Security Function

3 Access Control Policy

This section identifies the cryptographic keys and other Critical Security Parameters (CSPs) that the operator has access to while performing a service. It also defines the type(s) of access the operator has to the parameters.

3.1 Roles

The different roles are described in section 2.1.

3.2 Services

The CHR provides secure loading and storage of signed applications. In addition, the CHR offers the following services.

Role	*Authorized Services*	*Cryptographic Keys and CSPs*	*Access Type*
SO	Show Status	None	None
	Application & AP Public Key Load	RSA Public Key (CA)	Execute
	Zeroization	None	None
	On-Demand Self-Tests	None	None

Table 5 SO services

Role	*Authorized Services*	*Cryptographic Keys and CSPs*	*Access Type*
User	Application start	RSA Public Key (AP)	Execute

Table 6 User services

The Application & AP Public Key Load Service controls the loading of the application and the Application Provider Public Key. When an application is loaded, the Loader verifies the chain of signatures. If an error occurs during loading, the application is not loaded and the CHR reports the error to the User on the serial port and the display.

The CHR transfers the control to the application after its successful loading.

The Zeroization Service is automatically executed after successful loading of the application. Security Officer is able to show status by rebooting the device. The Status output consists of a Power LED and a two-line display. Self-test report is also printed on the serial port (Refer to §5.3 "Status output").

3.3 Cryptographic Keys and Critical Security Parameters

The CHR flash memory is loaded with the CA public key in clear-text. It is the responsibility of the CA to load the CA Public Key in the CHR memory (see section 2.1). The flash memory is protected by the physical security mechanisms described in section 4.1. However, disclosure of the CA public key shall not be considered as a security risk. The public key cannot be used for signing an application.

The signature of the Application is a security related data. However, it shall not be considered as a Critical Security Parameters (CSPs) as disclosing it is not a security risk.

There is no Critical Security Parameters (CSPs) associated to the CHR but the CHR Cryptographic Module offers a secure storage area for Critical Security Parameters (CSPs) of the loaded Application.

The following table summarizes the module's keys:

Key	Generation	Storage	Use	Role
CA Public Key RSA 2048	Outside of Module	Flash, write protected	Authenticate the Security Officer (AP Public key signature verification)	Security Officer
AP Public Key RSA 2048	Outside of Module	Flash, signed by CA private key	Authenticate the Application Provider (verification of the signature of the Application)	User

Table 7 Module Keys

4 Physical Security Policy

4.1 Physical Security Mechanisms

The CHR is a tamper-evident cryptographic module which includes an internal tamper-resistant secured module and cards inside. The extent of the cryptographic boundary is the tamper resistant, tamper responsive chassis. (The Red dotted box in Figure 2 represents the physical cryptographic boundary which is the chassis). While the internal tamper-resistant secured module provides an additional layer of physical security protection, this physical protection is not within the scope of the level 3 validation, and is not to be confused with the CHR module itself. The FIPS 140-2, level 3 physical security requirements are met at the outer chassis, despite the additional security provided by the internal secured module.

The cryptographic module is protected against intrusion. All the components are located in a metallic box equipped with intrusion detection mechanisms (uprooting and opening detectors). In addition, the cryptographic module is equipped with sensors that cannot be disabled: movement and impact sensors, temperature sensor, and voltage sensor.

The internal secured module is composed of one card supporting the main processor, a crypto-processor, the FPGA, and the memory. The internal secured module is potted with a hard epoxy resin and protected by an anti-intrusion film (Molex). As stated earlier, these measures were implemented to provide an additional layer of protection beyond the scope of the FIPS 140-2 level 3 being claimed.

The sensors and anti-intrusion film are managed by a dedicated security processor (PIC) that receives and analyses the signals and triggers security alarms A or B

The internal secured module manages two types of memory, a flash memory, and a SRAM memory.

The flash memory supports the bootstrap/loader, the CA public key and two areas for loading applications (“partition-A” and “partition-B”).

The secured SRAM memory is divided into two areas (“sec-memory A” and “sec-memory B”).

The following table contains the list of events that would zeroize “sec-memory A” or “sec-memory B”:

Event	Security Alarm	Zeroized sec-memory
Cover opening	B	B
Movement detection	B	B
Temperature out of range	A	A & B
Resistive film tamper	A	A & B
Voltages out of range	A	A & B
Internal reference voltage out of range	A	A & B
Module disconnection from the communication board	A	A & B
Abnormal Security microcontroller reset	A	A & B
Security microcontroller watchdog	A	A & B
Zeroization service automatically run after successful application load		A & B

Table 8 Security mechanisms

Critical Security Parameters (CSPs) of the loaded Application that are stored in Sec-memory-B are zeroized in response to any tamper detection. Sec-memory-A may be used to store less sensitive data such as public keys, certificates or event logs.

The following figure illustrates the CHR architecture.

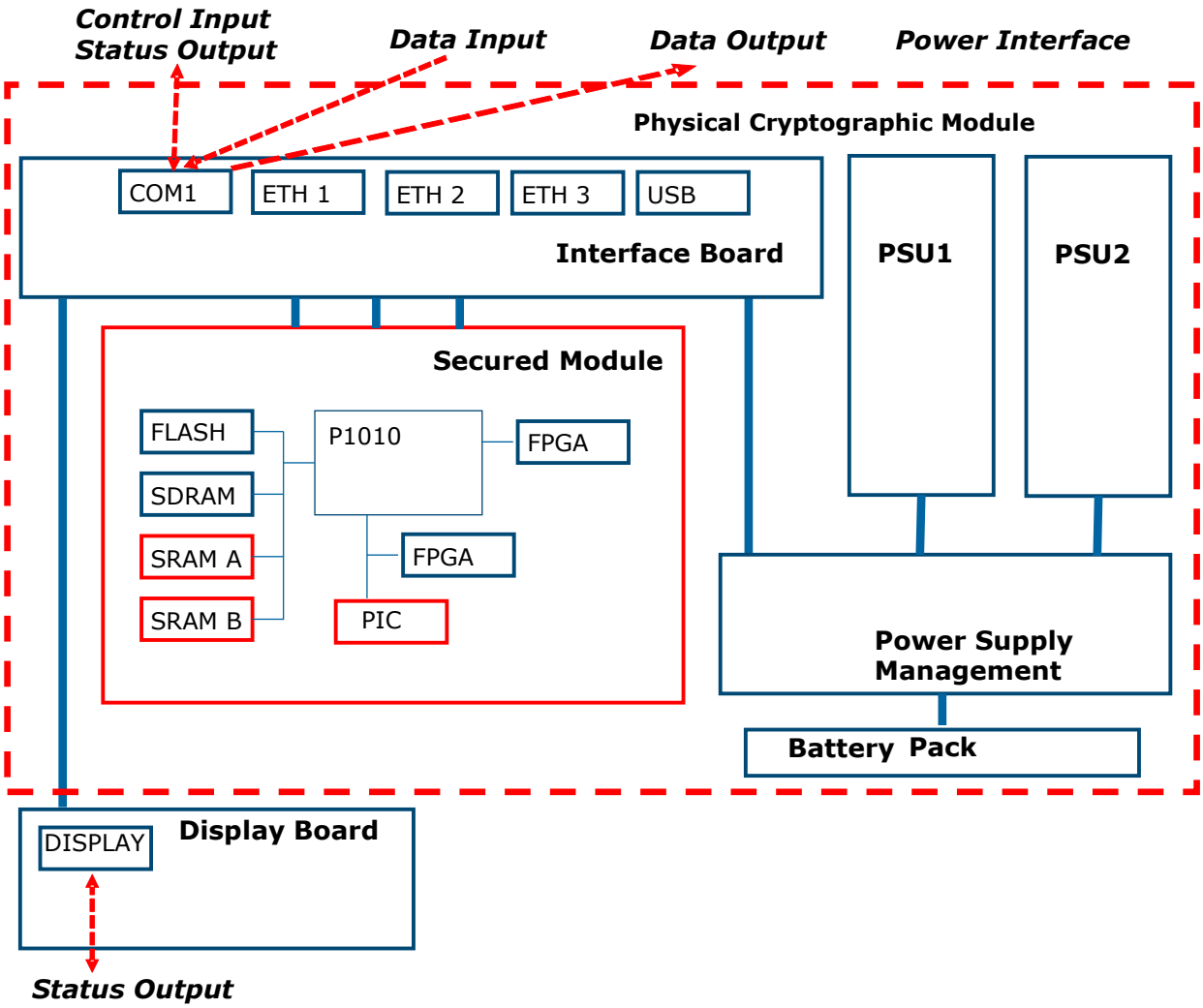

Figure 2 CHR Hardware Architecture

4.2 Physical Security Controls

In addition to the physical security mechanisms, the cryptographic module automatically performs several tests at power-up and when loading an application.

At power-up, the cryptographic module performs an automatic cryptographic algorithm test according to FIPS 140-2. In addition, the integrity of the firmware is checked. If one of these tests fails, the appropriate status is activated and the CHR is locked.

When loading an application, the chain of signatures (Application Provider and Certification Authority) is verified. If the verification fails, the application is not loaded, and the cryptographic module reports an error using the serial port.

5 Self-Tests

5.1 Self-Tests

The module performs the following self-tests at power on:

- Hardware tests (SRAM A, FPGA, SDRAM, SRAM B, FLASH)
- Firmware integrity test (SHA-256 digest verification).
- Cryptographic Algorithm Known Answer Test (RSA 2048 bit verify only and SHA-256 byte oriented).

In order to run self-tests on demand, it is necessary for the SO to reboot the module.

If one of these tests fails, a status message is printed before the CHR move to "Error" state (Refer to §5.3 Status output). The ERROR message is displayed in red.

The module is not capable of performing any cryptographic operation while in an error state.

In order to attempt to clear the error, the Security Officer must reboot the module. If the error persists, then the module should be returned to Atos for repair.

5.2 Conditional Tests

Both the Application start and Application load services include conditional tests performed sequentially:

- The Loader verifies a fixed header value,
- The Loader verifies the Application Provider's public key signature using the CA Public Key stored in the CHR.
- The Loader then verifies the application's signature using the Application Provider's public key.

To verify signatures, the Loader computes a hash using SHA-256 according to FIPS 180-4. The hash function is used by the RSA signature verification algorithm according to RSASSA-PKCS1-v1_5.

If one of these tests fails, a status message is printed before the CHR moves to "Idle" state to wait for another request (Refer to §5.3 Status output).

If all these tests pass, the application verification is successful.

5.3 Status Output

The power LED tells the operator that the module is receiving power.

All the possible ways that the two-line display shows status are listed below:

Display	Color	CHR state
Off		The power is off. Hardware security mechanism is still active
INIT	blue	Initializing the partitioning of memory and locking the first flash sector.
SELFTEST	blue	Performing self tests
WAIT COMMAND	blue	Waiting for SO instruction from the serial port
CHECK APP	blue	Checking the application to start
LOAD APP	blue	Loading a new application from input interface to SDRAM
	Green	Self test passed successfully - Application running
ZEROIZE	blue	Zeroizing SRAM memories
FLASH APP	blue	Flashing a new application from SDRAM to partition-A
ERROR	red	An error has been detected during self tests
SECURITY B	red	Security alarm B condition
SECURITY A	red	Security alarm A condition

Table 9 Messages on display

A self test report is printed on the serial port interface:

Hardware Tests:

Resource	Error message
SRAM A	SRAM A: ERROR
FPGA	FPGA: ERROR
SDRAM	SDRAM: ERROR
SRAM B	SRAM B: ERROR
FLASH	FLASH: ERROR

Software/Firmware Integrity Tests:

Integrity test	Error message
Firmware digest verification (SHA-256)	BOOTSTRAP INTEGRITY CHECK FAILED

Cryptographic Algorithm Known Answer Tests:

Algorithm test	Error message
RSA 2048 bit verify only	RSA KAT FAILED
SHA-256 byte oriented	SHA KAT FAILED

Tables 10 Self-test reports

When the self-test run successfully, the messages printed on the status output interface (serial port) are the following:
SRAM_A: OK
FPGA: OK
BCSR1: ####
SDRAM: OK
SRAM_B: OK
FLASH: OK
SHA KAT: OK
RSA KAT: OK
BOOTSTRAP INTEGRITY CHECK: OK

Conditional test report is printed on the serial port interface:

Conditional Test Result	Status Report
No valid information data	NO APP
Error during application header verification	APP HEADER CHECK FAILED
Error during application provider key verification	APP PROVIDER CHECK FAILED
Error during application signature verification	APP SIGNATURE CHECK FAILED
Application verified successfully	APP STARTED

Table 11 Conditional test reports

6 Security Officer and User Guidance

6.1 User Guidance

6.1.1 Module inspection

It is the user's responsibility to ensure that the module has not been tampered with by inspecting the two-line display and cover to ensure that it has not been damaged. The cover is locked with a pick resistant lock that cannot be opened by the end user. The lock can only be opened by the vendor at the manufacturing site. Lock and key are unique for each module.

Physical inspection (physical state, status display) should be performed once a month.

6.1.2 User's guide

Details on how to perform the user role securely are contained in the User's guide document [CHR/LP54040/EN]

6.2 Security Officer Guidance

6.2.1 Application signature

The secure loading of an application is activated after successful execution of the following steps that are outside of the scope of the Security Policy document.

1. The CA generates an asymmetric CA key pair.
2. The CA private key is used for public keys signature.
3. The CA public key is loaded on the CHR by the Security Officer.
4. The Application Provider generates an asymmetric AP key pair. The AP private key is used for signing the application.
5. The AP public key is sent to the CA.
6. The CA signs the AP public key with the CA private key and returns the signed key to the Application Provider.
7. The Application Provider signs the application with the AP private key,
8. The Application Provider adds the signed AP public key and the application signature to the application, thus creating an Application Load File.
9. The file is now ready to be loaded to the CHR module on behalf of the Security Officer

6.2.2 Security Officer's guide

Details on how to perform the Security Officer's role securely once the CHR is fielded are contained in the Security Officer's guide document [CHR/LP54025/EN]

7 Terminology and Bibliography

The following terms and references apply.

7.1 Glossary of Terms and Abbreviations

AP	Application Provider
CA	Certification Authority. In this document the CA is the entity responsible for generating the CA key pair. The CA private key is used for signing the Application Provider key and the CA Public Key is loaded in the CHR module.
CHR	CHR Cryptographic Module: Name of the Certified Platform
CSP	Critical Security Parameter
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DSA	Digital Signature Algorithm
DTA	Differential Timing Analysis
FLASH	Non-Volatile Re-Programmable Memory
FPGA	Field Programmable Gate Array
PIC	Security Processor
POE	Power Over Ethernet
SDRAM	Double Data Rate Synchronous Dynamic Random Access Memory
SRAM	Static Random Access Memory
USB	Universal Serial Bus

7.2 Bibliography

FIPS 140-2	Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules
FIPS 180-4	Federal Information Processing Standards Publication, Secure Hash Standard
FIPS 186-4	Federal Information Processing Standards Publication, Digital Signature Standard
CHR/LP54040/EN	CHR V006 User's Guide
CHR/LP54025/EN	CHR V006 Security Officer's Guide

END OF DOCUMENT