# Non-Proprietary FIPS 140-2 Security Policy

# for

# Zebra Technologies Corporation

# Zebra DCS Cryptographic Library

Firmware Module

Firmware Component Version:

DAACUS00-001-R00 – for STB3678, FLB3678 and CR8178
DAACVS00-001-R00 – for LI3678
DAACWS00-001-R00 – for DS3678 and DS8178

Document Version Number: 1.8

# 1. Module Description

The Zebra DCS Cryptographic Library provides data encryption/decryption functionality to devices such as wireless barcode scanners and cradles. These devices are used in a variety of environments such retails and manufacturing.

For the purposes of FIPS 140-2 the module is classified as a firmware module.

The main purpose of the module is to encrypt/decrypt data.

FIPS 140-2 conformance testing of the module was performed at Security Level 1. The following configurations were tested by the lab:

| **Firmware Component Version** | **Operating Systems** | **Hardware** |
|---|---|---|
| DAACUS00-001-R00.dal | uC/OS-II V2.85 | STB3678, FLB3678, and CR8178 |
| DAACVS00-001-R00.dal | uC/OS-II V2.85 | LI3678 |
| DAACWS00-001-R00.dal | TreadX V6.5 | DS3678 and DS8178 |

The following table summarizes FIPS 140-2 compliance claims

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

## 2. Cryptographic Boundary

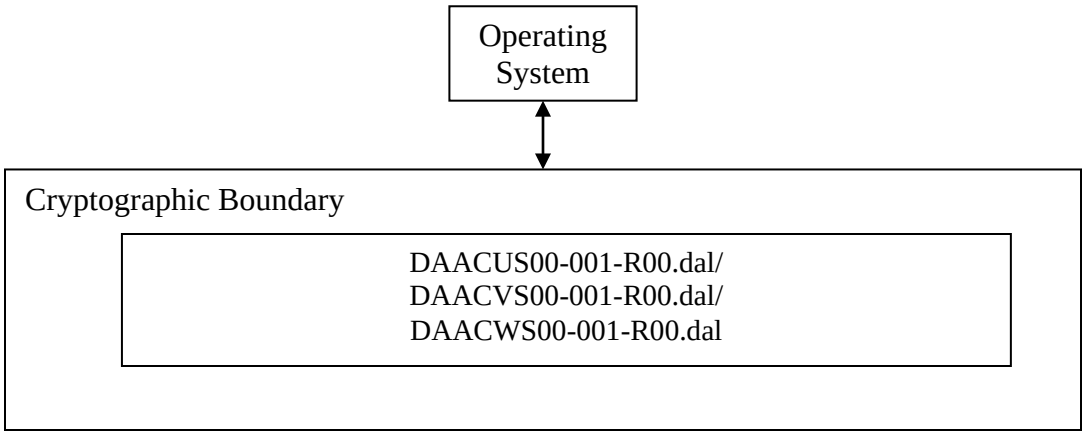
The cryptographic boundary of the module includes the firmware binary only.

The module includes the following logical interfaces:

- Control Input Interface: firmware API commands and command parameters used to control and configure module operation.
- Status Output Interface: return values from firmware API commands used to obtain information on the status of the module.
- Data Input Interface: data inputs to the firmware API commands
- Data Output Interface: data outputs of the firmware API commands

All module interfaces, inputs and outputs are provided by the firmware component.

Figure 1. Block Diagram



# 3. Roles and Services

The module provides the following roles:

1. User.
2. Crypto Officer.

The Crypto Officer configures the module and manages its cryptographic functionality. The User employs the cryptographic services provided by the module.

The module provides the following services to the User and Crypto Officer.

| Service | Role | Access to Cryptographic Keys and CSPs<br>R- read or use W – write or generate,<br>Z – zeroize<br>N/A – no CSPs are accessed by this service |
|---|---|---|
| Run-self tests | Crypto Officer/User | N/A |
| Get status of the module | Crypto Officer/User | N/A |
| Set AES key | Crypto Officer | W (sets AES encryption key) |
| Set shared encryption key | Crypto Officer | W (sets shared encryption key) |
| Encrypt/decrypt wireless data using the AES encryption key | User | R (uses the AES encryption key to encrypt/decrypt wireless data) |
| Encrypt/decrypt AES encryption key or the new shared encryption key using the current shared encryption key | User, Crypto Officer | R (uses the current shared encryption key to encrypt/decrypt the AES encryption key or the new shared encryption key) |
| Zeroize | Crypto Officer | Z (zeroizes all plaintext keys) |

The module is always in FIPS mode of operation; non-FIPS mode is not applicable.

# 4. Security Functions

The table below lists approved cryptographic algorithms employed by the module

| Algorithm | Certificate # |
|---|---|
| AES | #3856, #3857 and #3858 |
| HMAC | #2504, #2505 and #2506 |
| SHA-1 | #3178, #3179 and #3180 |

# 5. Key Management

The following cryptographic keys are supported by the module

| Name and Type | Generation or establishment | Usage |
|---|---|---|
| Access Key | Pre-set in the module binary | Read/Write AES and Shared keys from FLASH memory |
| AES encryption key | Loaded encrypted with the access key, or the shared key. | Encryption of the wireless data |
| Shared Key (Default) | Loaded encrypted with the access key. | Encryption of the AES key or the new Shared Key |
| Shared Key (Current) | Loaded encrypted with the previously established shared key. | Encryption of the AES key or the new Shared Key |
| HMAC SHA-1 integrity key | Pre-set in the module binary | Used to check integrity of the module at initialization |

To zeroize the keys inside the logical cryptographic boundary one shall execute Crypto_ClearAllKeys API function, which will zeroize all keys in RAM and in FLASH memory.

## 6. Self Tests.

The module runs a set of self-tests on execution of library load API call. If one of the self-tests fails, the module transitions into an error state, where all data output and cryptographic operations are disabled. The self-test success or failure is output as a return value of the library load API call.

The module runs self-tests for the following algorithms

| Algorithm | Test |
|---|---|
| AES | Known Answer Test (encrypt/decrypt) |
| SHA-1 | Tested during the integrity check |
| HMAC SHA-1 | Tested during the integrity check |

Note: The integrity check is done by computing the HMAC SHA-1 signature on the module binary and comparing it to the previously computed value. Therefore the requirement to self test HMAC and SHA-1 is fulfilled.

# 7. Approved Mode of Operation

The module always runs in the Approved Mode of Operation and does not implement any Non-Approved Security Functions. The module consists of production-grade components and meets FIPS 140-2 Level 1 physical security requirements.