FIPS-3 Security Policy Document

Authors: John Doe, Alice Green

Page 1

1. General

1.1 Overview

This document provides the non-proprietary security policy for the XYZ Cryptographic Module v1.0. The module implements FIPS 140-3 approved cryptographic algorithms and is designed for use in secure communication applications.

1.2 Security Levels

The module meets FIPS 140-3 Level 2 requirements for all security areas except physical security, which meets Level 1 requirements.

2. Cryptographic Module Specification

2.1 Description

The XYZ Cryptographic Module is a software-based cryptographic module that provides cryptographic services to applications. The module is implemented as a dynamic library that can be integrated into various software applications.

2.2 Tested and Vendor Affirmed Module Identification

The module has been tested on the following operating systems:

- Windows 10 (64-bit)
- Linux Ubuntu 20.04 (64-bit)
- macOS 12.0 (64-bit)

2.3 Excluded Components

No components are excluded from the cryptographic boundary.

3. Cryptographic Module Interfaces

Page 2

3.1 Ports and Interfaces

The module provides the following interfaces:

- Control Input Interface: API function calls
- Control Output Interface: API function responses
- Data Input Interface: Plaintext and ciphertext data
- Data Output Interface: Processed cryptographic data

4. Roles, Services, and Authentication

4.1 Authentication Methods

The module supports role-based authentication using API keys and digital certificates.

4.2 Roles

The module supports the following roles:

- Administrator: Full access to all module functions
- User: Limited access to cryptographic services

4.3 Approved Services

- Encryption/Decryption using AES
- Digital signature generation and verification
- Key generation and management

5. Software/Firmware Security

5.1 Integrity Techniques
The module uses digital signatures to ensure software integrity during loading and execution.

5.2 Initiate on Demand
Integrity checks are performed automatically when the module is loaded.

6. Operational Environment

6.1 Environment Type and Requirements
The module operates in a limited operational environment with the following requirements:
- Minimum 4GB RAM
- 500MB available disk space
- Network connectivity for certificate validation

7. Physical Security

7.1 Mechanisms and Actions Required
The module relies on the physical security of the host system. No specific physical security mechanisms are implemented by the module itself.

8. Non-Invasive Security

8.1 Mitigation Techniques
The module implements countermeasures against timing attacks and power analysis attacks.

9. Sensitive Security Parameters Management

9.1 Storage Areas
Cryptographic keys are stored in protected memory areas with appropriate access controls.

9.2 Input/Output Methods
Keys are input through secure API calls and output through encrypted channels.

10. Self-Tests

10.1 Pre-operational Tests
The module performs the following tests during initialization:
- Algorithm self-tests
- Integrity verification
- Random number generator tests

10.2 Conditional Tests
Conditional tests are performed when specific conditions are met, such as key generation or random number generation.

11. Life Cycle Assurance

11.1 Installation, Initialization, and Startup
The module includes detailed installation procedures and initialization requirements.

11.2 Administrator Guidance
Comprehensive administrator documentation is provided with the module.

12. Mitigation of Other Attacks

12.1 Attack List

The module provides protection against the following attacks:

- Timing attacks
- Power analysis attacks
- Fault injection attacks