# Defined Enforcement Rules (Informal)

Dhruv Sunil Bhatia
24CSB0A19
CSE - A
Q119 - Secure OTA Update Compiler

---

## 1 Overview

This section informally defines the security enforcement rules applied by the Secure OTA Update Compiler. These rules specify mandatory conditions that must hold on all control-flow paths leading to firmware installation. Violation of any rule results in compile-time failure.

## 2 Enforcement Rules

### Rule 1: Signature Verification Before Installation

Every execution path that reaches a firmware installation function must be preceded by successful cryptographic signature verification.

### Rule 2: Rollback Prevention via Version Monotonicity

Firmware installation is permitted only if the incoming firmware version is strictly greater than the currently installed firmware version.

### Rule 3: Trusted Update Source Validation

Firmware updates must originate from a trusted and authenticated source. Any update retrieved from an unverified or unauthenticated source is rejected.

### Rule 4: No Sensitive Information Leakage

Firmware update logic must not log or expose sensitive data such as cryptographic keys, firmware contents, or verification results during the update process.

### Rule 5: Approved Cryptographic API Usage

Only approved cryptographic primitives and APIs may be used for signature verification. Weak or deprecated algorithms are explicitly disallowed.