# CWE Detail – CWE-1267

## Description

The product uses an obsolete encoding mechanism to implement access controls.

## Extended Description

Within a System-On-a-Chip (SoC), various circuits and hardware engines generate transactions for the purpose of accessing (read/write) assets or performing various actions (e.g., reset, fetch, compute, etc.). Among various types of message information, a typical transaction is comprised of source identity (identifying the originator of the transaction) and a destination identity (routing the transaction to the respective entity). Sometimes the transactions are qualified with a Security Token. This Security Token helps the destination agent decide on the set of allowed actions (e.g., access to an asset for reads and writes). A policy encoder is used to map the bus transactions to Security Tokens that in turn are used as access-controls/protection mechanisms. A common weakness involves using an encoding which is no longer trusted, i.e., an obsolete encoding.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Related Attack Patterns (CAPEC)

* CAPEC-121
* CAPEC-681

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Modify Memory, Read Memory, Modify Files or Directories, Read Files or Directories, DoS: Resource Consumption (Other), Execute Unauthorized Code or Commands, Gain Privileges or Assume Identity, Bypass Protection Mechanism, Reduce Reliability — Notes:

## Potential Mitigations

**•** Architecture and Design: Security Token Decoders should be reviewed for design inconsistency and common weaknesses. Access and programming flows should be tested in both pre-silicon and post-silicon testing. (Effectiveness: High)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** The inherited policy encoding is obsolete and does not work for the new system where an untrusted bus master with an odd Security Token exists in the system, i.e., Master\_3 whose Security Token is "11". Based on the old policy, the untrusted bus master (Master\_3) has access to the AES-Key registers. To resolve this, a register AES\_KEY\_ACCESS\_POLICY can be defined to provide necessary, access controls: