# CWE Detail – CWE-1279

## Description

Performing cryptographic operations without ensuring that the supporting inputs are ready to supply valid data may compromise the cryptographic result.

## Extended Description

Many cryptographic hardware units depend upon other hardware units to supply information to them to produce a securely encrypted result. For example, a cryptographic unit that depends on an external random-number-generator (RNG) unit for entropy must wait until the RNG unit is producing random numbers. If a cryptographic unit retrieves a private encryption key from a fuse unit, the fuse unit must be up and running before a key may be supplied.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-97

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: The decision to continue using a cryptographic unit even though the input units to it are not producing valid data will compromise the encrypted result.

## Common Consequences

**•** Impact: Varies by Context — Notes:

## Potential Mitigations

**•** Architecture and Design: Best practices should be used to design cryptographic systems. (Effectiveness: N/A)

**•** Implementation: Continuously ensuring that cryptographic inputs are supplying valid information is necessary to ensure that the encrypted output is secure. (Effectiveness: N/A)

## Applicable Platforms

**•** Verilog (Class: None, Prevalence: Undetermined)

**•** VHDL (Class: None, Prevalence: Undetermined)

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

## Demonstrative Examples

**•** In the example above, first a check of RNG ready is performed. If the check fails, the RNG is ignored and a hard coded value is used instead. The hard coded value severely weakens the encrypted output.