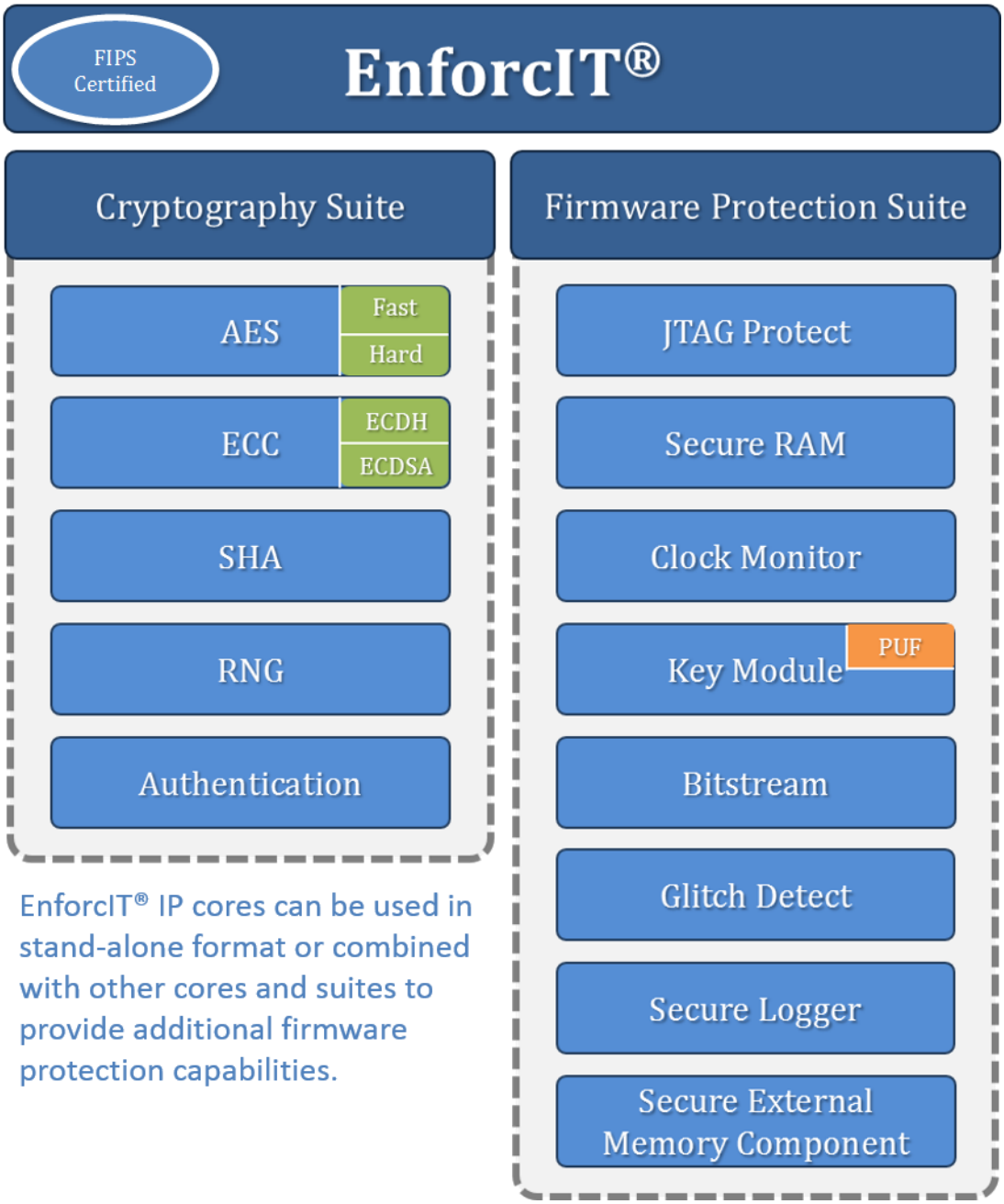

EnforcIT is a collection of FPGA IP cores that a user can instantiate in a design to provide cryptographic processing capabilities and security to the FPGA. It is comprised of two distinct collections of IP cores targeted as NSA Suite B cryptographic co-processing and FPGA self-protection. The IP cores are design to be largely FPGA agnostic, only relying on specific FPGA architecture features when design optimizations can be obtained. All cores are provided as encrypted VHDL using the Synopsys Synplify tool suite.

EnforcIT® Cryptography Suite

The EnforcIT Firmware Cryptography Suite is a selection of IP cores to be used for implementing cryptographic operations in firmware. They are provided as standalone cores included in the EnforcIT® Cryptography Suite.

- AES -- The Advanced Encryption Standard (AES) is a cryptographic algorithm used throughout government and industry to protect sensitive information from exposure (see NSA Suite B). This core is FIPS certified under Validation# 2389 and 2390
- ECC -- The ECC core is a component capable of performing various elliptic curve cryptographic operations. The Elliptic Curve Arithmetic Unit (ECAU), a stand-alone IP core, enables ECDH over p256 (a 256-bit prime field recommended by NIST in FIPS 186-3). Elliptic Curve Digital Signature Algorithm (ECDSA) is FIPS certified under Validation# 393
- RNG -- The Random Number Generator is used to provide a source of entropy for designs that require it.
- SHA-2 -- The SHA component (SHAC) is an implementation of the secure hash algorithm described in NIST FIPS-180-3. The SHAC also supports the Keyed-Hash Message Authentication Code (HMAC) described in FIPS 198-1. Keyed-Hash Message Authentication Code (HMAC) is FIPS certified under Validation# 1466. Secure Hash Standard (SHS) is FIPS certified under Validation# 2035.
- Authentication Node -- This core provides the ability of system components (firmware or software nodes) to authenticate each other between a software or firmware endpoint.

EnforcIT® Firmware Protection Suite

The EnforcIT Firmware Protection Suite is a selection of IP cores to be used for implementing protections of customer IP in FPGAs. They are provided as standalone cores and are included in the EnforcIT Firmware Protection Suite package.

- JTAG Protection -- The JTAG protection IP provides disabling, monitoring, and authorized use of the JTAG port.
- Clock Monitor / Glitch Detection -- A clock protection component provides the ability to monitor a clock for tampering.
- Secure RAM Controller -- The Secure RAM Component (SRC) protects the contents of RAM within an FPGA.
- Key Module -- The Key Module allows the user to select from a variety of ways to store keys in a design, while providing a standard protocol for retrieving the data in the system at runtime.
- Oscillator -- The Clock Oscillator is an independent, free-running internal clock intended for use as a reference clock for the Clock Monitor or other FPGA logic.
- Bitstream Protection -- Bitstream Protection includes the combination of multiple EnforcIT components to provide a secured FPGA boot.
- Secure Logger -- The Secure Logger allows the user to log information to a location such that it is a one-way encryption that can only be decrypted after removal from the system.
- Secure External Memory Controller -- SEMC performs inline memory encryption using AES-XTS. The SEMC is highly-configurable and may be optimized for various size, throughput, and latency trade-offs.
- Anti-Counterfeiting -- To deter counterfeiting, a physically unclonable function (PUF) feature provides the user with a device-specific signature used to create an encryption key.