RN0002
Release Notes
Core3DES v3.2

Microsemi
a Microchip company

Microsemi Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
Email: sales.support@microsemi.com
www.microsemi.com

About Microsemi

Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Learn more at www.microsemi.com.

1 Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

1.1 Revision 4.0

Added PolarFire® SoC support.

1.2 Revision 3.0

Added RTG4™ support.

1.3 Revision 2.0

Repackage the core.

1.4 Revision 1.0

Added support for the ProASIC3 and ProASIC3E families.

Contents

Tables

2 Core3DES v3.2

These release notes accompany the production release of the Core3DES IP core version 3.2. This document provides details about the features and enhancements, system requirements, supported families, implementations, and known issues and workarounds.

2.1 Key Features

The following are the features:

- Compliant with FIPS PUB 46-3
- TECB (TDEA Electronic Codebook) Implementation per ANSI Standard X9.52
- Example Source Code Provided for TCBC, TCFB, and TOFB Modes
- 168-Bit Cipher Key (consisting of 56-bit cipher keys in 3 stages, with 24 additional parity bits)
- All Major Microsemi® Device Families Supported
- Parity Checking Logic for Cipher Key
- Encryption and Decryption Possible with Same Core
- 48-Clock Cycle Operation to Encrypt or Decrypt 64 Bits of Data
- Pause/Resume Functionality to Continue Encryption or Decryption at Will
- Provides Data Security within a Secure Microsemi FPGA

2.2 Supported Interfaces

No standard interface available.

2.3 Delivery Types

Core3DES is available with Obfuscated and register transfer level (RTL) licenses.

2.3.1 Obfuscated

Complete RTL code is provided for the core, enabling the core to be instantiated with SmartDesign. Simulation, Synthesis, and Layout can be performed with Libero® System-on-Chip (SoC) or Integrated Design Environment (IDE). The RTL code for the core is obfuscated and some of the testbench source files are not provided. Instead, they are precompiled into the compiled simulation library.

2.3.2 RTL

Complete RTL source code is provided for the core and testbenches.

2.4 Supported Families

- PolarFire® SoC
- PolarFire®
- RTG4™
- IGLOO® 2
- SmartFusion® 2
- IGLOO^{PLUS}
- ProASIC3L
- SX-A
- RTSX-S
- Axcelerator®
- RTAX-S
- ProASIC^{PLUS}®
- ProASIC®3
- ProASIC3E
- Fusion
- SmartFusion®
- IGLOO®
- IGLOOe

2.5 Supported Tool Flows

- Core3DES v3.2 requires Libero IDE software v9.2 or Libero SoC software v11.5.

2.6 Installation Instructions

The Core3DES CPZ file must be installed into Libero software. This is done automatically through the Catalog update function in Libero, or the CPZ file can be manually added using the **Add Core** catalog feature. Once the CPZ file is installed in Libero, the core can be configured, generated, and instantiated within SmartDesign for inclusion in the Libero project. For more information, see the *Knowledge Based article*.

To know how to create SmartDesign project using the IP cores, refer to *Libero SoC documents page* and use the latest SmartDesign user guide.

2.7 Documentation

This release contains a copy of the *Core3DES Handbook*. The handbook, describes the core functionality and gives step-by-step instructions on how to simulate, synthesize, and place-and-route this core, and also implementation suggestions. Refer to *Libero SoC documents page* for instructions on obtaining IP documentation.

For updates and additional information, visit the Intellectual Property pages on the Microsemi SoC Products Group website: visit:

http://www.microsemi.com/products/fpga-soc/design-resources/ip-cores.

2.8 Supported Test Environments

The following test environments are supported:

- VHDL user testbench
- Verilog user testbench

2.9 Resolved Issues in v3.2 Release

There were no software action requests (SARs) resolved. PolarFireSoC support is added.

2.10 Resolved Issues in v3.1 Release

Table 1, page 7 shows the software action requests (SARs) resolved in the v3.1 release of Core3DES.

Table 1 • **Resolved SARs in Core3DES v3.1**

SAR No.	Description
57410	Added RTG4 Support.

2.11 Resolved Issues in v3.0 Release

Table 2, page 7 shows the SARs resolved in the v3.0 release of Core3DES.

Table 2 • **Resolved SARs in Core3DES v3.0**

SAR No.	Description
11491	Typo on throughput calculation in the handbook that has been changed.
11499	PA3 netlist fails with user testbench. Current tool flow does not support netlist.
11735	Default netlist fails during user testbench simulation. Current tool flow does not support netlist.

2.12 Known Limitations and Workarounds

There are no known issues or workarounds for Core3DES v3.2 release.