Core3DES v3.1 Release Notes

These release notes accompany the production release of the Core3DES IP core version 3.1. This document provides details about the features and enhancements, system requirements, supported families, implementations, and known issues and workarounds.

Key Features

Core3DES v3.1 has the following 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

Supported Interfaces

No standard interface available.

Delivery Types

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

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.

RTL

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

Supported Families

- IGLOO®
- IGLOO2
- IGLOOe
- IGLOO^{PLUS}
- Fusion
- ProASIC®3
- ProASIC3E
- ProASIC3L

- Axcelerator®
- RTAX-S
- ProASIC$^{PLUS®}$
- RTSX-S
- SX-A
- SmartFusion®
- SmartFusion2
- RTG4™

Supported Tool Flows

- Core3DES v3.1 requires Libero IDE software v9.2 or Libero SoC software v11.5.

Installation Instructions

The Core3DES CPZ file must be installed into Libero SoC software. This is done automatically through the Catalog update function in Libero SoC, or the CPZ file can be manually added using the Add Core catalog feature. Once installed in the Libero SoC Catalog, the core can be instantiated and configured. For the RTL release version of the core, the FlexLM license must be installed and Libero IDE restarted before the core can be configured and generated within SmartDesign. Refer to the *Libero SoC online help* for further instructions on core installation, licensing, and general use.

Documentation

The release contains 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 implementation suggestions.

For more information about Intellectual Property, visit: http://www.microsemi.com/products/fpga-soc/design-resources/ip-cores. For updates and additional information about software, FPGAs, and hardware, visit: http://www.microsemi.com.

Supported Test Environments

The following test environments are supported:

- VHDL user testbench
- Verilog user testbench

Release History

Table 1 shows the release history for Core3DES v3.1.

Table 1. Release History

Version	Date	Changes
3.1	February 2015	Support for RTG4 family is added.
3.0	April 2009	Repackage the core.
2.1	July 2007	Added support for the ProASIC3 and ProASIC3E families.

Resolved Issues in v3.1 Release

Table 2 shows the software action requests (SARs) resolved in the v3.1 release of Core3DES.

Table 2. Resolved SARs in Core3DES v3.1

SAR No.	Description
57410	Added RTG4 Support.

Resolved Issues in v3.0 Release

Table 3 shows the SARs resolved in the v3.0 release of Core3DES.

Table 3. 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.

Known Limitations and Workarounds

There are no known issues or workarounds for Core3DES v3.1 release.

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace 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; security technologies and scalable anti-tamper products; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,400 employees globally. Learn more at **www.microsemi.com**.

Microsemi Corporate 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

E-mail: sales.support@microsemi.com

© 2015 Microsemi Corporation. All rights reserved. Microsemi and the Microsemi logo are trademarks of Microsemi Corporation. All other trademarks and service marks are the property of their respective owners.

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.