
Core3DES v3.0 Release Notes

These release notes are for the production release of Core3DES v3.0. They describe features and enhancements, information about system requirements, supported families, implementations, and known issues and workarounds.

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 Actel 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 Actel FPGA

Delivery Types

Core3DES is available with Obfuscated and RTL licenses

Obfuscated

Complete RTL code is provided for the core, enabling the core to be instantiated with CoreConsole or SmartDesign. Simulation, Synthesis, and Layout can be performed with Libero 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[®] FPGAs
- IGLOO^e FPGAs
- IGLOO PLUS FPGAs
- Fusion FPGAs
- ProASIC[®]3 FPGAs
- ProASIC3E FPGAs
- ProASIC3L FPGAs
- Axcelerator[®] FPGAs
- RTAX-S FPGAs
- ProASIC^{PLUS}[®] FPGAs
- RTSX-S FPGAs
- SX-A FPGAs

Supported Tool Flows

This version of the core requires the following tools:

- Libero IDE v8.4 or later
- CoreConsole v1.4 (optional)

Install Instructions

The Core3DES CCZ file can be installed using SmartDesign

Libero IDE/SmartDesign Instructions

Within Libero IDE, click the Add Core button in the Catalog to locate and install a local CCZ file, or use the automatic web update feature in Libero IDE. Once the CCZ file is installed in Libero IDE, the core can be instantiated, configured, and generated within SmartDesign for inclusion in your Libero IDE project.

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 IDE online help for instructions about core installation and licensing.

Documentation

This release contains a copy of the Core3DES handbook. The Core3DES handbook describes the core functionality, gives step-by-step instructions on how to simulate, synthesize, and place-and-route this core, and provides implementation suggestions. The documentation can be viewed by right-clicking the Core Selection window in CoreConsole after the core has been installed.

For updates and additional information about the software, devices, and hardware, visit the Intellectual Property pages on the Actel website at www.actel.com.

Supported Test Environments

- VHDL user testbench
- Verilog user testbench

Release History

Table 1 · Release History

Version	Date	Changes
3.0	April 2009	Repackage the core
2.1	July 2007	V2.1 adds support for the ProASIC3 and ProASIC3E families

Resolved Issues

Table 2 lists Software Action Requests (SARs) that were resolved in the v3.0 release of Core3DES.

Table 2 · Resolved Issues in the Core3DES v3.0 Release

SAR	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 with the Core3DES v3.0 release.

Actel and the Actel logo are registered trademarks of Actel Corporation.
All other trademarks are the property of their owners.



Actel is the leader in low-power and mixed-signal FPGAs and offers the most comprehensive portfolio of system and power management solutions. Power Matters. Learn more at www.actel.com.

Actel Corporation • 2061 Stierlin Court • Mountain View, CA 94043 • USA

Phone 650.318.4200 • Fax 650.318.4600 • Customer Service: 650.318.1010 • Customer Applications Center: 800.262.1060

Actel Europe Ltd. • River Court, Meadows Business Park • Station Approach, Blackwater • Camberley Surrey GU17 9AB • United Kingdom

Phone +44 (0) 1276 609 300 • Fax +44 (0) 1276 607 540

Actel Japan • EXOS Ebisu Building 4F • 1-24-14 Ebisu Shibuya-ku • Tokyo 150 • Japan

Phone +81.03.3445.7671 • Fax +81.03.3445.7668 • www.jp.actel.com

Actel Hong Kong • Room 2107, China Resources Building • 26 Harbour Road • Wanchai • Hong Kong

Phone +852 2185 6460 • Fax +852 2185 6488 • www.actel.com.cn