PKCS IP Core
Overview

V1.25.8 November 7th, 2025

Public-Key Cryptography
PKCS IP Core

Highlights

- Comprehensive implementation in accordance with RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, PKCS #5 v2.0
- Support for SHA256 algorithm
- Technology-independent HDL model
- Simple external interface for easy adaptation
- Structured core design
- Optimized for minimal area, low power consumption, and reduced computation time

Enhance your cryptographic solutions with our advanced and efficient PKCS IP.

Overview

The **PKCS IP** is specifically designed for RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, specifically PKCS #5 v2.0.

With its internal data memory block interface, the **PKCS IP** simplifies programming and execution, making it the ideal solution for your cryptographic needs.

Function

Main Building Blocks:

- Input Data Memory Interface
- Output Data Register Bank
- Program and Constant ROMs
- CoProcessor (with the Register Banks)

Experience seamless data exchange with our advanced PKCS IP.
By reading from external memory and writing results to a dual output register bank, our IP efficiently performs PKCS computations based on the hardwired program in the program ROM.
This ensures optimal performance and reliability for your cryptographic needs.

Functions available

- SHA256
- HMAC_SHA256
- PBKDF2
- KDF2

Functions with special requirements are available in a short time upon request (info@tes-dst.com).

Performance

PKCS CoProcessor

KDF2 using 33 iterations

XILINX ARTIC7:

- ~ 1,77 msec @ Fmax up to 40MHz

xFab 180nm:

- ~ 8,76 msec @ Fmax up to 8MHz

KDF2 using 3333 iterations

XILINX ARTIC7:

- ~ 177 msec @ Fmax up to 40MHz

xFab 180nm:

- ~ 876 msec @ Fmax up to 8MHz

Advantage

- Software-defined 256-bit implementation
- Customizable PKCS-specific user functions
- User requirements easily implemented through microcoding

Testing

The TES PKCS IP Core has successfully completed the Known Answer Test and Monte Carlo Tests as specified by NIST. These tests were conducted in ModelSim© and IKOS© Mode.

Additionally, eVerification© Tests against the Python Algorithm RTL Equivalence and the executable OpenSSL specification were performed at speed and across multiple instances.

The TES PKCS IP Core passed all Tests, demonstrating its reliability and performance.

Deliveries

- User-Documentation
- Encrypted VHDL RTL code

Applications

The NIS 2 Directive is crucial EU legislation designed to help enhance cybersecurity for operational technology (OT) systems in critical infrastructure, setting new standards across EU member states and promoting proactive measures to help improve business continuity and resilience against evolving cyber threats.

Examples:

- Industrial control
- Smart Home Applications
- IoT devices
- Protected Communication

Why TES Electronic Solutions PKCS Solution for Your Business

- Superior quality and efficient object codes
- Comprehensive services: product tuning, hardware and software optimization, and final product design support
- Leading IC chip design service provider
- Exceptional high-tech engineering service references

Elevate your projects with our top-tier solutions and expertise.

TES related IPs

- **AES Encryption and Decryption**
- **CAN / CAN FD**
  Controller area Network core including transfer and object layer.
- **MPEG-4**: Low Cost MPEG-4 for video coding
- **D/AVE Family**: Embedded graphic processing unit (GPU)

Contact

TES Electronic Solutions GmbH
Nikolaus-Otto-Straße 25
70771 Leinfelden-Echterdingen
Tel. +49 (0)711 / 214 74 0
E-mail: info@tes-dst.com
https://www.tes-dst.com