TI Software

Secure Hash Algorithm-1 (SHA-1)

Release Notes

Applies to Release: 1.0
Publication Date: October 21, 2008

Texas Instruments, Incorporated
20450 Century Boulevard
Germantown, MD 20874 USA

Contents

NOTICE OF CONFIDENTIAL AND PROPRIETARY INFORMATION

Information contained herein is subject to the terms of the Non-Disclosure Agreement between Texas Instruments, Inc. and your company, and is of a highly-sensitive nature. It is confidential and proprietary to Texas Instruments, Inc. It shall not be distributed, reproduced, or disclosed orally or in written form, in whole or in part, to any party other than the direct recipients without the express written consent of Texas Instruments, Inc.

Release Notes

SHA-1 1.0

Introduction

The SHA-1 component provides the Secure Hash Algorithm 1 for little and big endian processors. The component supports generation of a 160 bit message digest for input messages up to 2^64 bits.

License and Standard Information

Source information:

- The SHA-1 code provided within this package is based on the open source SHA-1 code provided by OpenSSL release 0.9.8h, which can be found at http://www.openssl.org/source/.

Standards information:

- The SHA-1 code provided within this package implements FIPS Standard 180-1 – Secure Hash Standard.
    - SHA-1 FIPS Standard
      http://www.itl.nist.gov/fipspubs/fip180-1.htm

Known Issues

None.

Documentation

The following documentation is available:

- SHA-1 Doxygen API Document
  sha1/docs/doxygen/SHA1API.chm

- SHA-1 Test Module Doxygen Document

sha1/test/docs/doxygen/SHA1_TEST.chm

- SHA-1 RFC 3174
  http://www.ietf.org/rfc/rfc3174.txt

New This Release

Current Changes

The following changes have been made in release 1.0.0.2:

- New SHA-1 algorithm based on OpenSSL implementation of SHA-1
- Two hashing algorithms provided per endian format
    - Speed algorithm
        - Based on OpenSSL “large footprint” implementation
        - Unrolls all loops in the hashing function to produce lower cycle counts
        - Consumes roughly twice the program memory of “size” implementation
    - Size algorithm
        - Based on OpenSSL “small footprint” implementation
        - Small program memory footprint
- SHA-1 unit test improvements
    - Improved accuracy of cycle measurements
    - Added ability to test multiple calls to sha1Update prior to calling sha1Final

Previous Changes

Release 1.0.0.1:

- Fixed bug preventing correct hash from being produced when a block of data is split and processed with two simultaneous calls to the sha1Update function.

Release 1.0.0.0:

- SHA1 authentication algorithm for c64x+ big and little endian targets
- Support for generation of 160 bit message digest
- Support for input messages up to 2^64 bits
- APIs in place to implement HMAC level optimization
    - Details can be found in the SHA1 API Doxygen document or in the HMAC RFC, http://www.ietf.org/rfc/rfc2104.txt

Upgrade and Compatibility Information

Compatibility Key Definitions

Compatibility keys are intentionally independent of Marketing product numbers and are intended to:

1. Enable tooling to identify incompatibilities between components, and
2. Convey a level of compatibility between different releases to set end user expectations.

Compatibility keys are composed of 4 comma-delimited numbers - M,S,R,P - where:

- **M = Major**. A difference in M indicates a break in compatibility.
- **S = Source**. A difference in S indicates source compatibility. That is, the user's source doesn't require change, but *does* require rebuilding.
- **R = Radix**. A difference in R indicates an introduction of new features, but compatibility with previous interfaces has not broken. If libraries are provided by the package, an application must re-link with the new libraries, but not rebuild from source.
- **P = Patch**. A difference in P indicates that only bugs have been fixed in the latest package and no new features have been introduced. If libraries are provided by the package, an application must re-link with the new libraries, but is not required to recompile its source.

Device Support

This release supports the following device families:

- C64P

Validation Information

This release was built and validated using the following:

Component Dependencies

SHA-1
- ti.mas.types 4.1.0.1 (Common data type definitions)
- ti.mas.secutil 1.0.0.0 (Common security utilities)
- ti.mas.swtools 3.1.0.2 (Internally used s/w tools)

SHA1 Test Simulation
- ti.mas.types 4.1.0.1 (Common data type definitions)
- ti.mas.secutil 1.0.0.0 (Security utilities)
- ti.mas.util 3.1.0.0 (Common utilities)
- ti.mas.sha1 1.0.0.1 (Secure Hash Algorithm 1 component to be tested)
- ti.mas.sdk 1.2.0.1 (test infrastructure software)

Tool Dependencies for Source Release

- XDCVERSION = xdc_3_00_04
- COVERITY VERSION = prevent-mingw-3.8.0
- C64 CODEGENVERSION = cgen6_0_15
- SDO ARCHITECTURE = sdoarch_standards_1_00_00_05

- XDAISVERSION = xdais_5_21
- XDCCGROOT = C:/tools/
- DOXYGENVERSION = 1.5.1-p1
- GRAPGVIZVERSION = 2.12
- HTMLHELPWORKSHOP = 10-01-2007
- TITEMPLATES = 10-01-2007

Benchmarks

The following benchmarks were taken for the release:

- For cycle and memory benchmarks of the SHA-1 algorithms please refer to the SHA-1 test simulation documentation link provided in the 'Documentation' section of this document. The cycle and memory data can be found under the 'Related Pages" tab.

Versioning

Version Information:

Version Information is composed of 4 comma-delimited numbers – V, R, X, P - where:

- **V = Version -** Substantial difference from the last release.
- **R = Revision** – Minor difference from the last release.
- **X = External Vertical –** Vertical specific release.
- **P = Patch -** For any release other than mentioned above.

Technical Support and Product Updates

Contact local TI Field Application Engineer for technical support.