TI Software

Secure Hash Algorithm-1 (SHA-1)

Release Notes

Applies to Release: 1.0
Publication Date: July 7, 2008

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

Contents

Release Notes

SHA-1 1.0

Introduction

The SHA1 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.

Documentation

SHA1 Doxygen API Document:
ti/mas/sha1/docs/doxygen/SHA1API.chm

SHA1 Test Module Doxygen Document:
ti/mas/sha1/test/docs/doxygen/SHA1_TEST.chm

SHA1 FIPS Standard:
http://www.itl.nist.gov/fipspubs/fip180-1.htm

SHA1 RFC Page
http://www.ietf.org/rfc/rfc3174.txt

New This Release

Initial release
- 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

The integrator should be aware an extra input parameter, over open source implementations, has been added to SHA1 Init function. The input parameter allows an HMAC implementation to pass it a pre-initialized SHA1 context structure for use in an HMAC level optimization. If the HMAC is not utilizing the optimization it should pass a NULL pointer for this parameter. More details can be found in the Doxygen documentation.

Device Support

C64x+ Targets
- Tomahawk (TCI 6486)
  - Big endian
  - Little endian
- Himalaya (TCI 6482, 6455) [not tested]
  - Big endian
  - Little endian

Validation Information

Component Dependencies

SHA1
- 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 1.0.0.0 (Secure Hash Algorithm 1 unit to be tested)
- ti.mas.sdk 1.2.0.1 (test infrastructure software)

Tool Dependencies

- XDCVERSION = xdc_3_00_04
- COVERITY VERSION = prevent-mingw-3.8.0
- C54 CODEGENVERSION = 4-10
- C55 CODEGENVERSION = cgen401
- 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

Compiler Options

Please view the SHA1 package.bld file located in ti/mas/sha1 directory.

Known Issues

None

Benchmarks

Benchmarks can be found in the SHA1 test simulation documentation located in the ti/mas/sha1/test/docs/doxygen/ directory. Memory and MIPS information can be found under the 'Related Pages" tab.

Versioning

The component version definition can be found at the following site under section 'Compatibility Keys and Version Numbers':
https://twiki.dal.design.ti.com/twiki/bin/view/ASP/DSPS/Germantown/GTComponentGuidelinesC2

Technical Support and Product Updates

Contact local TI Field Application Engineer for technical support.

AES component information can be found at the following location:
https://twiki.dal.design.ti.com/twiki/bin/view/ASP/DSPS/Germantown/TiMasSha1