

A study commissioned by the Federal Office for Information Security (BSI)

Project 197

Secure Implementation of a Universal Crypto Library

Test Report

Version 1.2.0
Botan 2.0.1-RSCS1



Summary

The objective of this project is the secure implementation of a universal crypto library which contains all common cryptographic primitives that are necessary for the wide use of cryptographic operations. These include symmetric and asymmetric encryption and signature methods, PRFs, hash functions and RNGs. Additionally, security standards such as X.509 and SSL/TLS have to be supported. The library will be provided to manufacturers of VS-NfD products which will help the Federal Office for Information Security (BSI) to evaluate these products.

This document reports the test results of the Botan test suite.

Authors

Daniel Neus (DN)

René Korthaus (RK)

Copyright

This work is protected by copyright law. Every application outside of copyright law without explicit permission by the Federal Office for Information Security (BSI) is forbidden and will be prosecuted. This holds especially for the reproduction, translation, microfilming and storing and processing in electronic systems.

Secure Implementation of a Universal Crypto Library

Test Report
Botan Version 2.0.1-RSCS1

Changelog

Version	Authors	Comment	Date
1.0.0	DN, RK	Initial version	2016-11-11
1.1.0	RK	Update to Botan 2.0.0	2017-01-09
1.2.0	DN	Update to Botan 2.0.1-RSCS1	2017-03-06

Table of Contents

1 Test Report.....9

1.1 Linux.....10

1.1.1 Clang 64 bit.....10

1.1.2 GCC 64 bit.....11

1.1.3 GCC 32 bit.....12

1.2 Windows.....13

1.2.1 Visual Studio 2013.....13

1.2.2 Visual Studio 2015.....14

1 Test Report

The following report lists the test results for the Botan test suite. The following information is given for each test run:

- Information about the test environment
 - Botan configuration
 - Date and time of execution
 - Operating system
 - Compiler and compiler version
 - Target architecture
- Number of tests executed
 - Of these, the number of tests executed successfully
 - Of these, the number of failed tests
- A list of failed tests and the reason for each test failure

1.1 Linux

1.1.1 Clang 64 bit

Test Environment	
Botan Configuration	<code>./configure.py --module-policy=bsi --enable-modules=tls,pkcs11,xts --cc=clang --cc-bin=clang++ --with-bzip2 --with-lzma --with-sqlite --with-zlib</code>
Test Command	<code>./botan-test --run-long-tests --run-online-tests ./botan-test --pkcs11-lib=/path/to/SoftHSMv2 pkcs11</code>
Execution Date	2017/03/05
Operating System	Ubuntu 16.04, 64 bit
Compiler Version	clang version 3.8.0-2ubuntu4 (tags/RELEASE_380/final)
Architecture	x86_64
Test Results	
Tests Executed	424106
Successful Tests	424106
Failed Tests	0

1.1.2 GCC 64 bit

Test Environment	
Botan Configuration	./configure.py --module-policy=bsi --enable-modules=tls,pkcs11,xts --cc=gcc --cc-bin=g++ --with-bzip2 --with-lzma --with-sqlite --with-zlib
Test Command	./botan-test --run-long-tests --run-online-tests ./botan-test --pkcs11-lib=/path/to/SoftHSMv2 pkcs11
Execution Date	2017/03/05
Operating System	Ubuntu 16.04
Compiler Version	g++ (Ubuntu 5.4.0-6ubuntu1~16.04.4) 5.4.0 20160609
Architecture	x86_64
Test Results	
Tests Executed	424105
Successful Tests	424105
Failed Tests	0

1.1.3 GCC 32 bit

Test Environment	
Botan Configuration	./configure.py --module-policy=bsi --enable-modules=tls,pkcs11,xts --cpu=x86 --cc-abi-flags=-m32 --cc=gcc --cc-bin=g++ --with-bzip2 --with-lzma --with-sqlite --with-zlib
Test Command	./botan-test --run-long-tests --run-online-tests
Execution Date	2017/03/05
Operating System	Ubuntu 16.04
Compiler Version	g++ (Ubuntu 5.4.0-6ubuntu1~16.04.4) 5.4.0 20160609
Architecture	x86
Test Results	
Tests Executed	424016
Successful Tests	424016
Failed Tests	0

1.2 Windows

1.2.1 Visual Studio 2013

Test Environment	
Botan Configuration	./configure.py --module-policy=bsi --enable-modules=tls,pkcs11,xts --cc=msvc --cpu=x86
Test Command	./botan-test --run-long-tests --run-online-tests ./botan-test --pkcs11-lib=/path/to/SoftHSMv2 pkcs11
Execution Date	2017/03/05
Operating System	Windows 7
Compiler Version	Visual Studio 2013
Architecture	x86
Test Results	
Tests Executed	424002
Successful Tests	424002
Failed Tests	0

1.2.2 Visual Studio 2015

Test Environment	
Botan Configuration	./configure.py --module-policy=bsi --enable-modules=tls,pkcs11,xts --cc=msvc --cpu=x86
Test Command	./botan-test --run-long-tests --run-online-tests ./botan-test --pkcs11-lib=/path/to/SoftHSMv2 pkcs11
Execution Date	2017/03/05
Operating System	Windows 7
Compiler Version	Visual Studio 2015
Architecture	x86
Test Results	
Tests Executed	424000
Successful Tests	424000
Failed Tests	0