The RSASP1 Signature Primitive Validation System (RSASP1VS)

Updated: June 16, 2014
Updated: March 18, 2014
Original: January 8, 2013

Sharon S. Keller

National Institute of Standards and Technology
Information Technology Laboratory
Computer Security Division
TABLE OF CONTENTS

1 INTRODUCTION ........................................................................................................................................... 1
2 SCOPE ......................................................................................................................................................... 1
3 CONFORMANCE ........................................................................................................................................... 1
4 DEFINITIONS AND ABBREVIATIONS ............................................................................................................. 2
  4.1 DEFINITIONS ........................................................................................................................................ 2
  4.2 ABBREVIATIONS ................................................................................................................................. 2
5 DESIGN PHILOSOPHY OF THE RSASP1 PRIMITIVE VALIDATION SYSTEM ............................................. 2
6 RSASP1VS TESTS .......................................................................................................................................... 3
  6.1 CONFIGURATION INFORMATION ......................................................................................................... 3
  6.2 THE RSASP1 TEST ............................................................................................................................ 3
APPENDIX A REFERENCES .............................................................................................................................. 5
Update Log

06/16/14
• Change reference of CAVS to RSASP1VS.

01/16/14
• Removing the need to specify between PKCS1.5 and PKCS PSS. Was testing more than just the RSASP1 function. This function only tests the modular exponentiation function.
• Specify that “The format of the input message is not specified or tested by this validation test.”

09/05/13
• Updated References to FIPS 186-4 throughout document.
1 Introduction

This document, RSASP1 Signature Primitive Validation System (RSASP1VS), specifies the procedures involved in validating implementations of the RSASP1 signature primitive specified in Section 5.2 of the PKCS#1 v2.1: RSA Cryptography Standard (June 14, 2002) [1]. This primitive is used by both the RSA SSA-PKCS1-v1_5 and the RSA SSA-PSS signature schemes referenced in FIPS186-4, Digital Signature Standard (DSS) [2] and specified in [1]. The validation testing of the RSASP1 primitive validates the correctness of the exponentiation function portion of the signature generation function.

The RSASP1VS is designed to perform automated testing on Implementations Under Test (IUTs). This document provides the basic design and configuration of the RSASP1VS. It defines the purpose, the design philosophy, and the high-level description of the validation process for the RSASP1 signature primitive. The requirements and procedures to be followed by those seeking formal validation of an implementation of the RSASP1 primitive are presented. The requirements described include the specification of the data communicated between the IUT and the RSASP1VS, the details of the tests that the IUT must pass for formal validation, and general instruction for interfacing with the RSASP1VS.

A set of RSASP1 primitive test vectors is available on the http://csrc.nist.gov/groups/STM/cavp/index.html website for testing purposes.

2 Scope

This document specifies the validation tests required to validate IUTs for conformance to the RSASP1 primitive utilized by both the RSA SSA-PKCS1-v1_5 and the RSA SSA-PSS signature schemes. The RSASP1 primitive performs the exponentiation function resulting in the signature. In applications using PIV cards, this exponentiation function is performed on the card. The RSASP1VS provides testing to determine the correctness of the implementation of the primitive. It determines if the RSASP1 implementation produces the expected signature by performing the modular exponentiation. The format of the input message is not specified or tested by this validation test.

3 Conformance

The successful completion of the validation test contained within the RSASP1VS is required to claim conformance to the RSASP1 primitive. Testing for the cryptographic module in which the application-specific algorithm is implemented is defined in FIPS PUB 140-2, Security Requirements for Cryptographic Modules [3].
4 Definitions and Abbreviations

4.1 Definitions

<table>
<thead>
<tr>
<th>DEFINITION</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>CST laboratory</td>
<td>Cryptographic Security Testing laboratory that operates the RSASP1VS</td>
</tr>
<tr>
<td>IUT</td>
<td>Implementation Under Test</td>
</tr>
<tr>
<td>PKCS</td>
<td>Public Key Cryptography Standards</td>
</tr>
</tbody>
</table>

4.2 Abbreviations

<table>
<thead>
<tr>
<th>ABBREVIATION</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANS</td>
<td>American National Standard</td>
</tr>
<tr>
<td>RSASP1VS</td>
<td>RSASP1 Signature Primitive Validation System</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>IUT</td>
<td>Implementation Under Test</td>
</tr>
</tbody>
</table>

5 Design Philosophy of the RSASP1 Primitive Validation System

The RSASP1VS is designed to test conformance to specifications in Section 5.2 of PKCS#1 v2.1 rather than provide a measure of a product’s security. The validation tests are designed to assist in the detection of accidental implementation errors, and are not designed to detect intentional attempts to misrepresent conformance. Thus, validation should not be interpreted as an evaluation or endorsement of overall product security.

The RSASP1VS has the following design philosophy:

1. The RSASP1VS is designed to allow the testing of an IUT at locations remote to the RSASP1VS. The RSASP1VS and the IUT communicate data via REQUEST (.req) and RESPONSE (.rsp) files. The RSASP1VS also generates SAMPLE (.sam) files to provide the IUT with an example of the RESPONSE file format.
2. The testing performed within the RSASPV1VS uses statistical sampling (i.e., only a small number of the possible cases are tested); hence, the successful validation of a device does not imply 100% conformance with the Recommendation.

6 RSASPV1VS Tests

When applied to an IUT, the RSASPV1VS provides testing to determine the correctness of the RSASP1 function. The RSASPV1VS consists of a single validation test.

6.1 Configuration Information

To initiate the validation process of the RSASPV1VS, a vendor submits an application to an accredited laboratory requesting the validation of its implementation of the RSASP1 Signature component. The vendor’s implementation is referred to as the Implementation Under Test (IUT). The request for validation includes background information describing the IUT along with information needed by the RSASPV1VS to perform the specific tests. More specifically, the request for validation includes:

1. Cryptographic algorithm implementation information
   
   a) Vendor Name
   
   b) Implementation Name;
   
   c) Implementation Version;
   
   d) Indication if implemented in software, firmware, or hardware;
   
   e) Processor and Operating System with which the IUT was tested if the IUT is implemented in software or firmware;
   
   f) Brief description of the IUT or the product/product family in which the IUT is implemented by the vendor (2-3 sentences);

6.2 The RSASPV1 Test

The RSASPV1 test generates one request (.req) file: RSASPV1.req.

Each file begins with a header that has the CAVS Tool version on line one, the name of the test and the RSA algorithm being tested - “RSASPV1” and the implementation name on line two, and the modulus size tested on line three. Line 4 displays the date the file was generated. Line 5 is the mod size being tested in square brackets. This is always mod = 2048 for this component test.

# CAVS 14.1
# "RSASPV1" information for "testPSS"
# Combination tested: Mod Size 2048
# Generated on Thu Oct 11 09:06:27 2012
RSASP1VS generates 30 trials. Each trial, or count, has the following format:

\[
\text{COUNT} = 0
\]
\[
n = a63fb6b665165b254ed49b84bfdb1912d900eb55d302a649c55a5640533c4bc22ace842e2ff7d3
\]
\[
d = 1635d1dafa93ea4dbab196c0799f79e352a487626f389cd180075d8ad1a59161692675499c1c65e14f3fe5
\]

RSASP1VS supplies the modulus \( n \), the private key \( d \), and a random message \( m \). The values are represented in hexadecimal. The sample file indicates the outputs that the IUT needs to provide.

\[
\text{COUNT} = 0
\]
\[
n = a63fb6b665165b254ed49b84bfdb1912d900eb55d302a649c55a5640533c4bc22ace842e2ff7d3
\]
\[
d = 1635d1dafa93ea4dbab196c0799f79e352a487626f389cd180075d8ad1a59161692675499c1c65e14f3fe5
\]
The S value is the resulting signature from performing the exponentiation equation $s = m^d \mod n$ in the RSASP1 function. If the RSASP1 function fails, indicate $s = \text{FAIL}$. The RSASP1 function would fail if the value for $m$ is larger than the value for $n-1$. If this occurs, the first step in the RSASP1 function which states

1. If the message representative $m$ is not between 0 and $n-1$, output “message representative out of range” and stop.

would cause the signature to fail.

The RSASP1VS verifies the correctness of the IUT’s value of $s$ by comparing it to previously computed RSASP1VS values. If the resulting signatures match, then the IUT’s implementation of the RSASP1 function passes the validation test. If the values do not match, the IUT has an error in it. If an error occurs during validation, the values computed by the RSASP1VS and the IUT are written to the log file. The CST Laboratory can use the information in the log file to assist the vendor in debugging the IUT.

### Appendix A  References

