# ACVP KAS IFC SSC Specification

Russell Hammett
*HII Technical Solutions Division*
*302 Sentinel Drive, Suite #300, Annapolis Junction, MD 20701*

August 19, 2020

National Institute of
Standards and Technology
U.S. Department of Commerce

## Abstract

This document defines the JSON schema for testing KAS-IFC-SSC SP800-56Br2 implementations with the ACVP specification.

## Keywords

The following are keywords to be used by search engines and document catalogues.

ACVP; cryptography

## Foreword

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

## Audience

This document is intended for the users and developers of ACVP.

## Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 of [RFC 2119] and [RFC 8174] when, and only when, they appear in all capitals, as shown here.

## Acknowledgements

This document is produced by the Security Testing, Validation and Measurement group under the Automated Cryptographic Validation Testing (ACVT) program.

## Executive Summary

The Automated Crypto Validation Protocol (ACVP) defines a mechanism to automatically verify the cryptographic implementation of a software or hardware crypto module. The ACVP specification defines how a crypto module communicates with an ACVP server, including crypto

capabilities negotiation, session management, authentication, vector processing and more. The ACVP specification does not define algorithm specific JSON constructs for performing the crypto validation. A series of ACVP sub-specifications define the constructs for testing individual crypto algorithms. Each sub-specification addresses a specific class of crypto algorithms. This sub-specification defines the JSON constructs for testing KAS-IFC-SSC SP800-56Br2 implementations using ACVP.

## Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

## Additional Information

For additional information on NIST's Cybersecurity programs, projects and publications, visit the Computer Security Resource Center. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is also available.

## Feedback

Feedback on this publication is welcome, and can be sent to: code-signing@nist.gov.

# 1. Introduction

The Automated Crypto Validation Protocol (ACVP) defines a mechanism to automatically verify the cryptographic implementation of a software or hardware crypto module. The ACVP specification defines how a crypto module communicates with an ACVP server, including crypto capabilities negotiation, session management, authentication, vector processing and more. The ACVP specification does not define algorithm specific JSON constructs for performing the crypto validation. A series of ACVP sub-specifications define the constructs for testing individual crypto algorithms. Each sub-specification addresses a specific class of crypto algorithms. This sub-specification defines the JSON constructs for testing KAS-IFC-SSC SP800-56Br2 implementations using ACVP.

## 2. Supported KAS-IFC-SSC

The following shared secret computation and test revision pair **MAY** be advertised by the ACVP compliant cryptographic module:

- KAS-IFC-SSC / SP800-56Br2

# 3. Test Types and Test Coverage

The ACVP server performs a set of tests on the KAS protocol in order to assess the correctness and robustness of the implementation. A typical ACVP validation session **SHALL** require multiple tests to be performed for every supported permutation of KAS capabilities. This section describes the design of the tests used to validate implementations of KAS algorithms.

## 3.1. Test Types

There are two test types for KAS testing:

- "AFT" — Algorithm Function Test. In the AFT test mode, the IUT **SHALL** act as a party in the Key Agreement with the ACVP server. The server **SHALL** generate and provide all necessary information for the IUT to compute a shared secret `z`; both the server and IUT **MAY** act as party U/V.
- "VAL" — Validation test. In the VAL test mode, The ACVP server **MUST** generate a complete (from both party U and party V's perspectives) shared secret `z`, and expects the IUT to be able to determine if that shared secret is valid. Various types of conditions/errors **MUST** be introduced in varying portions of the key agreement process (changed Z, Z with leading zero nibble, etc), that the IUT **MUST** be able to detect and report on.

## 3.2. Test Coverage

The tests described in this document have the intention of ensuring an implementation is conformant to [SP 800-56B Rev. 2].

### 3.2.1. Requirements Covered

- SP 800-56Br2 — 5.3 Random Bit Generators. Though random values are used, the testing of the construction of those random values **SHALL NOT** be in scope of ACVP testing.
- SP 800-56Br2 — 6.2 Criteria for RSA Key Pairs for Key Establishment. The ACVP server **SHALL** support the three key generation methods of "basic", "prime factor", and "CRT".
- SP 800-56Br2 — 6.3 RSA Key-Pair Generators. The ACVP server **SHALL** utilize IUT provided RSA public keys, and generate key pairs to accommodate testing. The ACVP server **SHALL** support both fixed and random public exponents.
- SP 800-56Br2 — 7 Primitives and Operations. 7.1 Encryption and Decryption primitives as well as 7.2 Encryption and Decryption Operations **SHALL** be used for the calculation/validation of the shared secret `z`.
- SP 800-56Br2 — 8 Key-Agreement Schemes. ACVP server testing will make use of "KAS1" and "KAS2" for testing of shared secret `z`. These exact schemes are not specified in the document, as "-basic" and "*-confirmation" make use of at least a KDF, if not also Key Confirmation. The intention of testing against the algorithm described in this document is specifically around the calculation of the shared secret `z`.

### 3.2.2. Requirements Not Covered

- SP 800-56Br2 — 5.3 Random Bit Generators. Though random values are used, the testing of the construction of those random values **SHALL NOT** be in scope of ACVP testing.
- KAS SSC testing only covers testing of SP800-56Br2 through the computation of a shared secret $z$. Additional functions of KAS as a whole such as KDF, KC, etc. **MAY** be covered within the scope of the full KAS testing; please see that document for further details.

# 4. Capabilities Registration

ACVP requires crypto modules to register their capabilities. This allows the crypto module to advertise support for specific algorithms, notifying the ACVP server which algorithms need test vectors generated for the validation process. This section describes the constructs for advertising support of KAS-IFC-SSC SP800-56Br2 algorithms to the ACVP server.

The algorithm capabilities **MUST** be advertised as JSON objects within the 'algorithms' value of the ACVP registration message. The 'algorithms' value is an array, where each array element is an individual JSON object defined in this section. The 'algorithms' value is part of the 'capability_exchange' element of the ACVP JSON registration message. See the ACVP specification [ACVP] for more details on the registration message.

## 4.1. Prerequisites

Each algorithm implementation **MAY** rely on other cryptographic primitives. For example, RSA Signature algorithms depend on an underlying hash function. Each of these underlying algorithm primitives must be validated, either separately or as part of the same submission. ACVP provides a mechanism for specifying the required prerequisites:

Prerequisites, if applicable, **MUST** be submitted in the registration as the `prereqVals` JSON property array inside each element of the `algorithms` array. Each element in the `prereqVals` array **MUST** contain the following properties

**Table 1 — Prerequisite Properties**

| JSON Property | Description | JSON Type |
|---|---|---|
| algorithm | a prerequisite algorithm | string |
| valValue | algorithm validation number | string |

A "valValue" of "same" **SHALL** be used to indicate that the prerequisite is being met by a different algorithm in the capability exchange in the same registration.

An example description of prerequisites within a single algorithm capability exchange looks like this

```
"prereqVals":
[
  {
    "algorithm": "Alg1",
    "valValue": "Val-1234"
  },
  {
    "algorithm": "Alg2",
    "valValue": "same"
  }
```

```
]
```

**Figure 1**

## 4.2. Prerequisite Algorithms

Some algorithm implementations rely on other cryptographic primitives. For example, IKEv2 uses an underlying SHA algorithm. Each of these underlying algorithm primitives must be validated, either separately or as part of the same submission. ACVP provides a mechanism for specifying the required prerequisites:

**Table 2 — Prerequisite Algorithms JSON Values**

| JSON Value | Description | JSON Type | Valid Values | Optional |
|---|---|---|---|---|
| algorithm | a prerequisite algorithm | value | DRBG, RSA | No |
| valValue | algorithm validation number | value | actual number or “same” | No |
| prereqAlgVal | prerequisite algorithm validation | object with algorithm and valValue properties | see above | Yes |

KAS has conditional prerequisite algorithms, depending on the capabilities registered:

**Table 3 — Prerequisite requirement conditions**

| Prerequisite Algorithm | Condition |
|---|---|
| DRBG | Always **REQUIRED** |
| SHA | Always **REQUIRED** |
| RSA | RSA KeyGen validation **REQUIRED** when IUT makes use of the generation/validation of keys within the module boundary. |

## 4.3. Algorithm Capabilities JSON Values

Each algorithm capability advertised is a self-contained JSON object using the following values.

**Table 4 — KAS ECC Capabilities JSON Values**

| JSON Value | Description | JSON Type | Valid Values | Optional |
|---|---|---|---|---|
| algorithm | The algorithm under test | value | KAS-IFC-SSC | No |
| revision | The algorithm testing revision to use. | value | “Sp800-56Br2” | No |

| JSON Value | Description | JSON Type | Valid Values | Optional |
|---|---|---|---|---|
| prereqVals | Prerequisite algorithm validations | array of prereqAlgVal objects | See Section 4.2 | No |
| keyGenerationMethods | The supported key generation methods. | array of string | See Section 4.4 | No |
| modulo | The supported common modulo | array of integer | See Section 4.5 | No |
| fixedPubExp | The fixed public exponent used for key generation. Required if using at least 1 static fixed public exponent key generation method. | hex | | Yes |
| scheme | Array of supported key agreement schemes each having their own capabilities | object | See Section 4.6.1 | No |

Note: Some optional values are **REQUIRED** depending on the algorithm. Failure to provide these values will result in the ACVP server returning an error to the ACVP client during registration.

### 4.4. Supported Key Generation Methods

At least one key generation method is **REQUIRED** within the array. The following types **MAY** be advertised by the ACVP compliant crypto module:

- rsakpg1-basic — An RSA key pair with a private key in the basic format, and with a fixed public exponent.
- rsakpg1-prime-factor — An RSA key pair with a private key in the prime factor format, and with a fixed public exponent.
- rsakpg1-crt — An RSA key pair with a private key in the Chinese Remainder Theorem format, and with a fixed public exponent.
- rsakpg2-basic — An RSA key pair with a private key in the basic format, with a random public exponent.

- rsakpg2-prime-factor — An RSA key pair with a private key in the prime factor format, with a random public exponent.
- rsakpg2-crt — An RSA key pair with a private key in the Chinese Remainder Theorem format, with a random public exponent.

### 4.5. Supported Common Modulo

At least one supported common modulo is **REQUIRED** within the array. The following common modulo **MAY** be advertised by the ACVP compliant crypto module:

- 2048 — estimated security strength 112
- 3072 — estimated security strength 128
- 4096 — estimated security strength 152
- 6144 — estimated security strength 176
- 8192 — estimated security strength 200

#### 4.5.1. Hash Function Z

An optional hash function that should be applied to `z` from both the ACVP server and IUT for comparison purposes. The provided `hashFunctionZ's security strength **MUST** be at least as strong as the greatest security strength modulo selected from Section 4.5

The following hash functions **MAY** be advertised by an ACVP compliant server:

- SHA-1
- SHA2-224
- SHA2-256
- SHA2-384
- SHA2-512
- SHA2-512/224
- SHA2-512/256
- SHA3-224
- SHA3-256
- SHA3-384
- SHA3-512

### 4.6. KAS IFC Schemes

All other scheme capabilities are advertised as a self-contained JSON object using the following values. Note that **AT LEAST** one valid scheme must be registered.

### 4.6.1. KAS IFC Scheme Capabilities JSON Values

KAS Schemes

- KAS1
- KAS2

**Table 5 — KAS IFC Capabilities JSON Values**

| JSON Value | Description | JSON Type | Valid Values | Optional |
|---|---|---|---|---|
| kasRole | Roles supported for key agreement | array | initiator and/or responder | No |

## 4.7. Example Registration

The following is a example JSON object advertising support for KAS IFC SSC.

```
{
  "vsId": 0,
  "algorithm": "KAS-IFC-SSC",
  "revision": "Sp800-56Br2",
  "scheme": {
    "KAS1": {
      "kasRole": [
        "initiator",
        "responder"
      ]
    },
    "KAS2": {
      "kasRole": [
        "initiator",
        "responder"
      ]
    }
  },
  "keyGenerationMethods": [
    "rsakpg2-basic",
    "rsakpg2-crt"
  ],
  "modulo": [
    2048
  ],
  "hashFunctionZ": "SHA2-512"
}
```

**Figure 2**

## 5. Generation Requirements per Party per Scheme

The various schemes of KAS/KTS all have their own requirements as to keys and nonces per scheme, per party. The below table demonstrates those generation requirements:

**Table 6 — Required Party Generation Obligations**

| Scheme | KasMode | KasRole | KeyPair | Generates Cipher Text |
|---|---|---|---|---|
| KAS1 | NoKdfNoKc | InitiatorPartyU | False | True |
| KAS1 | NoKdfNoKc | ResponderPartyV | True | False |
| KAS2 | NoKdfNoKc | InitiatorPartyU | True | True |
| KAS2 | NoKdfNoKc | ResponderPartyV | True | True |

# 6. Test Vectors

The ACVP server provides test vectors to the ACVP client, which are then processed and returned to the ACVP server for validation. A typical ACVP validation test session would require multiple test vector sets to be downloaded and processed by the ACVP client. Each test vector set represents an individual algorithm defined during the capability exchange. This section describes the JSON schema for a test vector set used with KAS-IFC-SSC SP800-56Br2 algorithms.

The test vector set JSON schema is a multi-level hierarchy that contains meta data for the entire vector set as well as individual test vectors to be processed by the ACVP client. The following table describes the JSON elements at the top level of the hierarchy.

**Table 7 — Top Level Test Vector JSON Elements**

| JSON Values | Description | JSON Type |
|---|---|---|
| acvVersion | Protocol version identifier | string |
| vsId | Unique numeric vector set identifier | integer |
| algorithm | Algorithm defined in the capability exchange | string |
| mode | Mode defined in the capability exchange | string |
| revision | Protocol test revision selected | string |
| testGroups | Array of test groups containing test data, see Section 6.1 | array |

An example of this would look like this

```
{
  "acvVersion": "version",
  "vsId": 1,
  "algorithm": "Alg1",
  "mode": "Mode1",
  "revision": "Revision1.0",
  "testGroups": [ ... ]
}
```

**Figure 3**

## 6.1. Test Groups JSON Schema

The testGroups element at the top level in the test vector JSON object is an array of test groups. Test vectors are grouped into similar test cases to reduce the amount of data transmitted in the vector set. For instance, all test vectors that use the same key size would be grouped together. The Test Group JSON object contains meta data that applies to all test vectors within the group. The following table describes the secure hash JSON elements of the Test Group JSON object.

The test group for KAS/KTS IFC is as follows:

**Table 8 — Vector Group JSON Object**

| JSON Value | Description | JSON Type | Optional |
|---|---|---|---|
| tgId | Numeric identifier for the test group, unique across the entire vector set. | value | No |
| testType | The type of test for the group (AFT or VAL). | value | No |
| scheme | The scheme in use for the group. See Section 4.6.1 for possible values. | value | No |
| kasRole | The group role from the perspective of the IUT. | value | No |
| keyGenerationMethod | The private key generation method for the group. | value | No |
| modulo | The modulo in use for key generation. | value | No |
| tests | The tests for the group. | Array of objects, See Section 6.2. | No |

## 6.2. Test Case JSON Schema

Each test group contains an array of one or more test cases. Each test case is a JSON object that represents a single test vector to be processed by the ACVP client. The following table describes the JSON elements for each KAS/KTS IFC test vector.

**Table 9 — Test Case JSON Object**

| JSON Value | Description | JSON Type | Optional |
|---|---|---|---|
| tcId | Numeric identifier for the test case, unique across the entire vector set. | value | No |
| serverN | RSA N value for the ACVP server's key. | value | Yes |
| serverE | RSA E value for the ACVP server's key. | value | Yes |
| serverP | RSA P value for the ACVP server's key. | value | Yes |

| JSON Value | Description | JSON Type | Optional |
|---|---|---|---|
| serverQ | RSA Q value for the ACVP server's key. | value | Yes |
| serverD | RSA D value for the ACVP server's key. | value | Yes |
| serverDmp1 | RSA Dmp1 value for the ACVP server's key. | value | Yes |
| serverDmq1 | RSA Dmq1 value for the ACVP server's key. | value | Yes |
| serverIqmp | RSA Iqmp value for the ACVP server's key. | value | Yes |
| iutN | RSA N value for the IUT's key. | value | Yes |
| iutE | RSA E value for the IUT's key. | value | Yes |
| iutP | RSA P value for the IUT's key. | value | Yes |
| iutQ | RSA Q value for the IUT's key. | value | Yes |
| iutD | RSA D value for the IUT's key. | value | Yes |
| iutDmp1 | RSA Dmp1 value for the IUT's key. | value | Yes |
| iutDmq1 | RSA Dmq1 value for the IUT's key. | value | Yes |
| iutIqmp | RSA Iqmp value for the IUT's key. | value | Yes |
| serverC | The ciphertext generated by the ACVP server, encrypted with the IUT's public key. | value | Yes |
| iutC | The ciphertext generated by the IUT, encrypted with the ACVP server's public key. | value | Yes |
| | The shared secret $z$. | value | Yes |
| hashZ | the shared secret $z$ after being run through the registered hash function (when applicable). | value | Yes |

### 6.3. Example Test Vectors JSON Object

The following is a example JSON object for test vectors sent from the ACVP server to the crypto module.

```
{
  "vsId": 0,
  "algorithm": "KAS-IFC-SSC",
```

```
 "mode": "",
 "revision": "Sp800-56Br2",
 "isSample": true,
 "testGroups": [
   {
     "tgId": 1,
     "testType": "AFT",
     "tests": [
       {
         "tcId": 1,
         "serverN":
"C649AC045BB1DBF46E4C03F2F89218D0431E5CAEF2E5287DC999A2D6AEA6378CBC537EB1C4D2F35EEC902AED
         "serverE": "0231E30EA607"
       },
       {
         "tcId": 2,
         "serverN":
"FC86CCE925571F96C86DD5DE5051CD5BA10EC97CF0951E674A1C44448E3E185F963B16BA366EA3BDAF6E48CA
         "serverE": "312C39FF83"
       },
       {
         "tcId": 3,
         "serverN":
"CBEA97A18EADA539F3383DCC9AD14D53F2347D0297BEBBF10D95D4A97846A3E86B1D23A227EC7F3DADD6F7BE
         "serverE": "028BB17DED"
       },
       {
         "tcId": 4,
         "serverN":
"A3145C5D1334185949F916B976A0F434CB0A964A4296259F4B67D70C014138EF23421A833409F002721158C0
         "serverE": "0198629BE7"
       },
       {
         "tcId": 5,
         "serverN":
"9C7102B454557D79BA2BBA2724B6CDBE1DF53270BBBA72FFB1BC41FB33278C7DBFB8CB7910CC27369C3F7704
         "serverE": "0530D5B083E1"
       }
     ],
     "scheme": "KAS1",
     "kasRole": "initiator",
     "keyGenerationMethod": "rsakpg2-basic",
     "modulo": 2048
   },
   {
     "tgId": 2,
```

```
      "testType": "AFT",
      "tests": [
        {
          "tcId": 6,
          "iutN":
"B1EC0D4310E9C1FDD3869552934A9A8AAF8D56481AD6DA9FB025E4411EE5D05F75BC7B8A59C84CF08A17A162
          "iutE": "0C4ACC1AB158D5",
          "iutP":
"BD1BFB5DE31BB6329BDCB5CF19D3EF092B1E030823AA5FEE7546C7535C9CD315EFF91A4F57EFC3F6BF9C349A
          "iutQ":
"F0DB0E710224CD6078B08F262914D3ADB75A327F4725DC0F0DA4E3C5658C4EEF843D6357AB048512551DB270
          "iutDmp1":
"0152F9A7453A909873978C1F8C80FEEC15E6E7794D2F2B51503BBEBB12B8E50D0F855FF826A836AC2A0D885B
          "iutDmq1":
"7088CE1732F6C77ACE5C5B83333017290B9FF202DD7207AFB11288D89D64E4924637027B1CB32E59B1E0B015
          "iutIqmp":
"7442F467D8ADE8E4E170B6836A1D520AE505AF84C3A74ECE0B7559E88091B0A0A6600011A5D065BC92A99A03
          "serverC":
"069891ACA1F6EBC1789DAC75696D347B0ADE86CCFA423A551736F2D79DB8194EDD91674392AD9E90E28ACFAB
        },
        {
          "tcId": 7,
          "iutN":
"9C737DC168F1F1C48F055EE0DEAF1B018AFDE9F1D3F79BD83066BACE6CF86B37E16ECD9688B0A9278DE4EB83
          "iutE": "3F6A2EE787",
          "iutP":
"D2569C32D3DDF20138536959DA14D1D6A50F37F6AB8EC409D0112552F548CD42E85BE5101DBFC6B89E764A61
          "iutQ":
"BE6A247849229A12F795ACDCC2A2E71CDA6A4EA8F37C7B0F2BB92558EE15896DBE29221AED41A0FB40C02B87
          "iutDmp1":
"C69C019BE0A4D0303238C812CB6D2081424BA282AADC3580AFD8CFB9FB8D29DE33E32A5F2CB7D7BC71FD8EF2
          "iutDmq1":
"60F45201E938A04CCB6235A64C14C533FBF6F59826C0189EA3A39C8279F5C12701AFA6D12DFCA9C9A8A7D7D7
          "iutIqmp":
"6E70C20E9FA4E6D6EE79B0AF9DD3E1DFAE4FD14CBB817D89421208E60E301EA60B9FAA4C1D72006988F36812
          "serverC":
"7FFBF0F3363435DD72DC5AE0560FFF63694A36D7D5431E92431B5F896750D85AF187BFA1812330C09DB06632
        },
        {
          "tcId": 8,
          "iutN":
"DC73CA09CBC5DF179D858DBE22076BA39B3D0653647C86476F5525DA3721650AD3C406CC701A1705E47F0FAE
          "iutE": "030BA3223807",
          "iutP":
"E680E1976429254F0F9159FD2069FCD3F1B7C2A9BA43137E46D7772502BFB8AC0A8A52DE5C3DF7D67331C059
```

```
          "iutQ":
"F4D64ABA36500B786E5CA91F2A4526753C5119B33CF6FD2E8BBA9301E39BFB9747867ED2FB89603748FC220B
          "iutDmp1":
"5DEB6D5833F48E28D62272F8F035BBB43B1C9B4B107C93C96406CB6ED36955D30B8D13DD6951AF76E55BF966
          "iutDmq1":
"657EFE3F0EFC609954394CD65AD414CF0F9B984C4932246195024CE8DE72B72F0F8F7C315549948E2D89551E
          "iutIqmp":
"8ABAB9429CC1701BB2C73C84F1D3687B5B26DA6695CE1714DE0D44FC5E0CE42F15FA40B2D790E1110F6F236E
          "serverC":
"C2EF3E526A11B413ABCB6DA03A1E0ECB882A1CB750327FA7FCC0C5196D5FD7AC50FE6A690F71DC67B6231F48
        },
        {
          "tcId": 9,
          "iutN":
"B43897D1D772D5A69C95F8E19B0A1AA6AFB05B084F458347E60E86092FD160174873AE20743C078842DCFD1D
          "iutE": "F7878E4B",
          "iutP":
"C6F76551221F1CE26E8F9F3724EB4269AF48CD73BDD1DF67D01156F05DED97A67D6770145D0B77C9C8379781
          "iutQ":
"E7E19F7DFF8F6F0FBFA30A37203D9D6609EA06B17D6FBEFD5036745BFBC2F32744CBF447918C0742C55AABBB
          "iutDmp1":
"B16178E54ECD8F8B7FD2188BD0CC088C127A9300C683E043BC4F058883C023B839510BB278E44AE4E5F1E913
          "iutDmq1":
"A87D125DED29B05035BA141CFF732C6EE40C0EC47FD1EC8C2DCF15427D833FE0ECE95439E852857A6FD1188F
          "iutIqmp":
"AEB85D2361C6B62F115E4BADE05E5C6E95B0B8B28B69D034FC74CFEE0FFF740BF7CB8D6480095E4CD37335DF
          "serverC":
"846AF208451055B128E45E8CA7A1021355E75261C0830DE1DE10CFBBC9A421B4D0690C1071B6346B3D907DAF
        },
        {
          "tcId": 10,
          "iutN":
"A4C62BAB1F1608417FC96DE24CEB9872823F5794B30FA1B2BDA7B3BC8B3F7791AC814EF5259151A55FB8BE5F
          "iutE": "3826704A0094CB",
          "iutP":
"BF1754F2A1643AEBA281D3816A3E745DC8323D115643439DE52FA5F3DE0BB6D942C58BFA7F717FFFF0A0439D
          "iutQ":
"DCBE64F1BE749E49F7EE1A9C11C5917A7ADC985384C3B9CFF1FD3B2AAA9718C9F37D5A84EA4DAFD4EC32C8B0
          "iutDmp1":
"B944CD247E11808AB70DF5D8CC989BE5EF16947B39E5547C53722B64CF88FB6725C1A641DB38FA76B9E3C4BE
          "iutDmq1":
"C64FEA3E7B6DFCA8448345729F15D952001240ACFA713300CD0399133B4281806BFCA4F229FC4A3112BE24CE
          "iutIqmp":
"8D542F8095B7D5242CC41320C35AE44347C309B1F8AA4944DE799891FF04E8335EBABC89454129B87B2638E5
          "serverC":
"3BA7202966866FB7160F765D62F9CA2DE6562CC3305ED980B0BAD2F0171839D3416178F96D126C406C0B85EE
```

```
        }
      ],
      "scheme": "KAS1",
      "kasRole": "responder",
      "keyGenerationMethod": "rsakpg2-crt",
      "modulo": 2048
    },
    {
      "tgId": 3,
      "testType": "AFT",
      "tests": [
        {
          "tcId": 11,
          "serverN":
"A5190DAE218D317D982FB55D4FFAD47A3B17AC5036722FCD69F1FF1BEF5F2518A1F64915B555A0D1E48AFF0A
          "serverE": "030B9D3C5085",
          "iutN":
"C17BFA0CB30157C5863B134FC54B1228729AD3C58BDDF7DCBD22B4CE60D05E4C0437AC44F4C23D2F09E48ABD
          "iutE": "1DD5284215FBC3",
          "iutP":
"C9302682794FDD67411550D1F18789C68D7C38970388C890E08D4522AF32605720A9971FEF5E59E510CFA222
          "iutQ":
"F632866BA4FE10774A2C456788F490E03FCCBBC05489FFA2E4F1090FA38968D8E702B2D95D6455DAB0365DC5
          "iutDmp1":
"4CA7D2DB266C26751AC3B2A3378C9610780F694F05AA096FB62D01B6EE43511C3F3A9B0D07D13532F234C400
          "iutDmq1":
"09C7D64D0BB7E2B306B6291AECD3D590E83A60E7FE4506D14B5978107F6C5FE08EDF3ECCFF724C129EAF3DBB
          "iutIqmp":
"62FFF4DB3D1CAC31D96D915E3ED7647BFC56CB1AA495D6533074AA814B355F78D282180AFD846AAD18FEEC20
          "serverC":
"0D7B9BD9D4F0C3F535F96274D19947E3D31F58E7C028DEFB8FBE1EDFC880CFCBC1FD745009BD6DD8A5F282DD
        },
        {
          "tcId": 12,
          "serverN":
"CBA17BEFB936219F26552CF3300FB04462CED5F74BAB0D7C83119D7FCF69BC290406942E665AFAD376ED2B3D
          "serverE": "8F3A4290F8FB",
          "iutN":
"9789F91B414D69DFDCFB593B52B775D86EB81ED89EB70BC44CDA1E5E5480D7813ED63C3C6BC7CBE8F556DFB4
          "iutE": "16FC9FFA65",
          "iutP":
"BADCAD3A43AAC5957A63951A35ED19DEA176BC07C77BE2B8BDC5A68E33B5A2820BD6102957EEDC341317A7E4
          "iutQ":
"CF9B8AF2E699588C9236A318CDDA2990B2F83B19653E0B0ACA45C951B66D4954B7F1709B98FC6798E50C6F59
          "iutDmp1":
"2D6389E47E9587A55F676C1EB19E4B443357229108EF8D1F468C6F65A1835E9152E475F117C6D13D57740190
```

```
        "iutDmq1":
"20D67C8A5F18A91236861E90EA448ED46254C875B2844B1C0BC64C138410B5FCB389C43A3E077EA5EA1C1C3F
        "iutIqmp":
"3002444807B4BD9E97CC954611E70AD76BD2AB4DDD9598B42E4F5E929FDA25BA6A98E78504E0BA21F82CF75A
        "serverC":
"6FE4B3C1E522FC2460FE4EAF833A537D91EC8FBD5D689E06EBE3CAE9D17E10CECFF7A633E291DFCDC2F43222
      },
      {
        "tcId": 13,
        "serverN":
"ED38C01CCB8CC8864823B02FCD3F010D54B68729E22C5DDD6206074D16BF65B79907C605BE7C74D51906F85D
        "serverE": "2CEF2F27C7",
        "iutN":
"D0FC83AE2B1D932556E34A8FC96328A8B853C124A8EC9C0DE46FD832EBBEBF5F950A15F24582917E7441188B
        "iutE": "2ABDDA9CB2D9F9",
        "iutP":
"EBE12582822FA5ACAD0CF31456B2EC1D007BCC752B905F0533BFBF97ADDD3D593A05BD295999F3DF7ED2AC41
        "iutQ":
"E2D01BD241A9582858F76D5A3FF7C3FBE2CD5BA82143A56DA45F58399666BE98702FA220D18AF4F701CE3E20
        "iutDmp1":
"DDB460A2CCD66164AB3CEAA77B7A1967DADBF0B45FFE5C3460D07251C3344562E9FD16A25C1EC50D9DB9976F
        "iutDmq1":
"4B5A3EBA708AA8608DCD7ED1EF3B75F7B2204CE5880760732EC418895C4A6B4E2ADE68AFDAFE25D83729EB5A
        "iutIqmp":
"D036D99E2DCF42E132C849B037C2CA66F1D0BDFA631E4D36D0ED17D59FB0B80D96385813C8A43462BE385FCA
        "serverC":
"992F52408CCB9591B0F0AD41F20ADE603C07923523C4D7DB39268CB1D2F2718D398A594580EB9B5E4361CD8C
      },
      {
        "tcId": 14,
        "serverN":
"F17F01349D4A4F421D098D60C287F13A7CB5DF4589D359485715018E6B2B353550A6AEA92B207BC638D95FEF
        "serverE": "013EC24CC95D",
        "iutN":
"9E6AABE068ADD486018F845FEF23FCCBC6DF66AA2A47C876A268758376EAFB70F93F1C62508A81D63BE72AE5
        "iutE": "9F5420E1",
        "iutP":
"C00826B4D74077E4ADBE5CCC0984E897724DBAF0E565011E184351A91062058C465865B7348FF4B31BB02BAB
        "iutQ":
"D32FEDEE3B86805A3FEE9BB832EDBD5919FBF949CEC43A8BE330F0BA585E4FA04A4EFEA5433DAA52A451FED3
        "iutDmp1":
"3C5A083F7C9F759EBF6A98AB33C30742597859509CB96E7C2944445B41E607CC4E37FF5664F6E2626C9B169B
        "iutDmq1":
"1274853EE6E0CBC6940EF0540E9FD6E6DD53FC3E1CD62A78AE29449D229470D3528EDECCD74AF1F75C4C4DA9
        "iutIqmp":
"8B05596B27893F86DC1AC0DA6E971C1B8D00DFE15140E350EB5F9AFC380EC59AC36FD49E140FFD87BAB6F32C
```

```
        "serverC":
"179FC4F05B58479D783BCF4AF04C64C358DFEEF9E0166578E0BD25F7BCB8250AA385E825A55C012BF7FF79EF
      },
      {
        "tcId": 15,
        "serverN":
"C8DEAF8CFA0E44632C9E440647C60A53BB4161C17B5230095FD16C0C7B9230ADCCF1C12DC0E165B71B2C0085
        "serverE": "8A2191B117",
        "iutN":
"EA347558C8FBE7EFA3C0E6C44F7CDF991990F8B533B4C5421531787DE9F99580A059780A791189A95CE99A32
        "iutE": "3750559C9E0223",
        "iutP":
"F64DAC64879F231FB36CD06265F8C9B3635B2B30CD51BC613D568DA67158C158D929FCFD53DEAC6864225D94
        "iutQ":
"F36CDA3479DFC5E6F4FDC447085F9AB4D0ED4422C6907EAEE753424C13167A9F3912662EA87A4E9D113B1AD8
        "iutDmp1":
"E5F9472AEF7723214253333659F936A36B3DFFA67388FEB41F15F1883C4D3977CD5251CDCB0E899F04EAA27B
        "iutDmq1":
"B8093F44CE2D14DFB942FB28624B001A301EA7731482D2D72B4A357E30418A857DE2B6CC8CFB988ECA9782A7
        "iutIqmp":
"27E3F554C904BCE6DC3415520168443051C0D4877EB98B58134C96CAE4366B30005E7A5CA1FCA3D8468A27BF
        "serverC":
"0115AF0B717EAE46FBB8801427C6124AD90661141AAC876EB96850C8A45655CD30F75D2E1885E7EB69A5B4FD
      }
    ],
    "scheme": "KAS2",
    "kasRole": "responder",
    "keyGenerationMethod": "rsakpg2-crt",
    "modulo": 2048
  },
  {
    "tgId": 4,
    "testType": "AFT",
    "tests": [
      {
        "tcId": 16,
        "serverN":
"B7E7C39FE9915DA23641D5EE0BBB54614734DF56AD9EA2EC4CEA4E30F96D781B144AA82F79182ED804AEA6CA
        "serverE": "8B09F449",
        "iutN":
"97CF55D43E6A58221AB79D6A2589E8F63D61E5C5E5A8779D6861B7A31CF4420BED958D72423B0F16E19FA554
        "iutE": "08510ECACB6D",
        "iutP":
"CB1FA795A1DDA64D65898D196DD1488929ECEF6222455B0F8795419461F7C11A82D1D8D6839955A575EFC387
        "iutQ":
"BF5415F0BE77B513906E7078DDA4641CF9AB390DB532681DA3E9B4D85DC197D1E3EA1FC27E29611BEEDB6C4F
```

```
        "iutD":
"1ECF01F8DF7EF993DCDA48640E66EB2947E32BA09DEFF5D70883A1DF271062001FA7DE3D1BC93D0F0E80CDA3
        "serverC":
"0D5BEF152B411E4D332110C3938970F824213238DD5AAACA4FFE46ED4F4134D73C32200FB48DCDFBB58FA39A
      },
      {
        "tcId": 17,
        "serverN":
"D21BE677FB589A161C09BC94507F374C502E9121DBA5BC909394AF9FEE73152750E662A15C49CF9C71C4DEC2
        "serverE": "0C9C0AC653A6AB",
        "iutN":
"A0B236E0681E10093525BA433B193B11CE79F460A800F5126FBD807CBAF172C57B18AD253CF49151A2C5B2C7
        "iutE": "375B397203",
        "iutP":
"CAA8B3D48EC1AD4BA106EECEF9AF2C8D173937FA3941F1C1D267980BA7125A8D72B4735CCD5D71BAAA10CD55
        "iutQ":
"CAFE07113D35DEBF8CFD35E97BCF5B1B94821AED0395C11C21126C755015839D6840E438B586961AF186BDF1
        "iutD":
"11087A573FC0FA01724F5DB3DBAA9C721B583905D29991C4CCAE6C81061C5CFE2DE0096121A0C58BFA70B900
        "serverC":
"88A8CC2220D03ACE7D6A84E3271F9D7FCF97CCDEF23D0EF8925090A2BA389D97F825F557848655EC438DEB67
      },
      {
        "tcId": 18,
        "serverN":
"A9A9EFBB78AC89103034B5F5951F04FB5B739FD82F37DAA271C1BBC836CDDDAE6CB875FEA6A44F838A6122E2
        "serverE": "3EB0ACCE483697",
        "iutN":
"B1FC89795C537CBC63109FC5F40F7A221C8FC3CEF64FC6FFC921A1C2097E454FD6362F924EF22577546AC37C
        "iutE": "C2436CDA2B6B",
        "iutP":
"BFD1D0A9947906455D1FE878E8CBA974E383C222565E877C509B13F0F376A18067AA8A5F1A57063CB45629A7
        "iutQ":
"ED89DAE440D094371AAE3349DE23C84E3D0EF6B34E3B817017285ED5DC140877FADEE0FD8D9DF8887A0150B4
        "iutD":
"22B345F1E7F73208278BCBE34C9F9650B46BAE81C70290EA6E7890DCC6C616FD36A9689A4EF1112CFDA64D6B
        "serverC":
"A6B136260D0FC4C9A6528608539E3BF5C2DBA4133A1BF7D5397DB1B1C4A1EAC2201643120DFC8ED37EEB20FC
      },
      {
        "tcId": 19,
        "serverN":
"AF2BF74AB07323FF2B75D4966581DA13A4EBCEDF1E1E390B845107989288576659A58A9D7939409CF9A35C25
        "serverE": "054F150537FBCB",
        "iutN":
"DC8766D9DDFE7DA342EFE6CFD92C19D36908638C1A2BE3A78134DFFD2E674707759916C7591DBE274D95F5D5
```

```
          "iutE": "07D50D7C506F",
          "iutP":
"E66B84D1804E268B26851FD25B9782F67904C754340EDDEF7F33C389BBCF0988D30CF3066373E16F2A388D7B
          "iutQ":
"F502C7DF099F479D50980D2B9E4D1A3231B24DE56E5F528CA4096B4680520DCE0683396AD9914BA69CD99B2A
          "iutD":
"1CFCB9253ED73F7B40B23E63954F3E4187784AE42D206DAC1EC7A0C9AA47976CF78381DA9A9C66963F25D67C
          "serverC":
"92F89B4EA7261E2B8F7D0B17FA961E054B1CFD034B36E88D29659CF60AD4C2C81F9FC2326BA35341E071E6BC
        },
        {
          "tcId": 20,
          "serverN":
"B979BCC97A10F7C26C49C128FFB994DDD264E848B6B4513B95827F3C2CBA3A8365C29CBC23D011E3270EE6EF
          "serverE": "0E34589343",
          "iutN":
"C20F6E1636C7C36343B4661BFBA27002EA0E798144912AC9E13C9AB1DC10E5B25DD01FE3C577D0CFCD1AEFBF
          "iutE": "2B08E7B5B5",
          "iutP":
"ED7CC2C218E7FBD7CAFC2241C3D75EC8DDC62BA263C11C8CA6B8780A083EFC5C0432D89D70261AC359F3EC36
          "iutQ":
"D1300C9A904EF9DC0E69718E8565173A25161C972AAB94BB5E4B0CD162B28F0CD1819818118486F2650301AA
          "iutD":
"0F82AF943057E2FEFE85BEA1DDF44B234E4BC450F618FE6B00E5FA1B3E9A7C326DD7D5149B8217BB89166DA6
          "serverC":
"40449B78E14703B6CA7002C1FA1DAD8DDA178D8E316E3139A913377C56FADFE776ACB79296F30C77BDCDEF8C
        }
      ],
      "scheme": "KAS2",
      "kasRole": "initiator",
      "keyGenerationMethod": "rsakpg2-basic",
      "modulo": 2048
    },
    {
      "tgId": 5,
      "testType": "VAL",
      "tests": [
        {
          "tcId": 21,
          "iutN":
"BDC5D92400652D7AF9FD836A92BAEF5F1139BA6366B8F03054237B8289BA07C6A0CE858EA6DA23FFA9BED12B
          "iutE": "05EC809FF3",
          "iutP":
"F060B8FFC67A5D9465F064D9254167CD1665FE5E646AD08BB2C7001791C1843D417D6EDBEB34C0036E77408D
          "iutQ":
"CA1B2FE2BF1E1570C30CDA4A98AE81B0AF0A0CBC81DF12CB29CDE7032C8B5C73E095535F60F4C7CA76C4E438
```

```
          "iutDmp1":
"CDCB518A278DB9F0DA611E1246BE27E6EB588061133C976A1DD11DD98F9E910CC2C2CCF57DC4D5B282DE0C20
          "iutDmq1":
"A221DFD1ED7C8415FBCA4AB986C6EA451E0505F3B492F384438EA071DF7A0751E7A6B1FDB95597D3283B3D32
          "iutIqmp":
"0EBC92C259B7895BC423FEB6568D4B9BB689EE0AF82463F7548749459CC8FAB23578F68A6063E14D4CBDD2CF
          "serverC":
"47BD46DC429D32A50441156A214190D93C2E8B3C8C7C72BF33356AB8457FD31B81CC964CCB083B6FB9CBE4D2
          "hashZ":
"1DFBD004D8B1B0ABF1F2225F916FE5F6E099B40917EB14150CE02F342BC302239FE12837634F5564E345B5DA
        },
        {
          "tcId": 22,
          "iutN":
"A0F6824EB13A551AE9061ECACA582F61178DDC0031D28776BCCC57835E9EB1AD004E05EA0C428FE01CC6EED3
          "iutE": "0C51DEF221",
          "iutP":
"D70805BE2CFEAD3991EF29E5A8CF2C59B06C48B86A537D86C470F63089F1C13CDD8C8AA9E91BEB439F202736
          "iutQ":
"BFA158125FDB6044D3B0C4948C5264D2EAE0EC66BE45CC42E576F283BF7E9195C4B41BD7492BF3D6004F6870
          "iutDmp1":
"7C584E6E3FC8054B442760F1D77AFE6BE9CA7F25B2016CC7F860D55032ECECC8BD625578CE524122F09FE461
          "iutDmq1":
"86C066BF24A3AD485F29C1F87134A6B08B78BC057219EDEFBE18D83245F52E73666BC39070AB3BE7AFB9F4BF
          "iutIqmp":
"1D92980D3AC7CE954962E764724BC2E17FD9014AC4AF0BD97F1AE77E926FE35D728547B5E72C349207E35CE8
          "serverC":
"8185C283C492BB449C916F1F0DFBDEC4B6722CEF320AC4748FACE01E1696CA83FA34431C4FA076E6FE234A6B
          "hashZ":
"65692B9528951BB6C6806C4A3EEAEE89A472693A42C39319F444ECAFCCF5BEE73197DC05A07B5598323DB21D
        },
        {
          "tcId": 23,
          "iutN":
"A4DE49BF9AFB58D4A4B2EC212A88977CC31E7BC766334B88B42D2D3837D690B77DF96E26CB25BF98BC92020D
          "iutE": "5CD5B42E17",
          "iutP":
"BC446DD1CE0BB7103272F38A1F18C6BEE7A0FA0814C86C10108A658567F25086AFD9A853B9CAB29E4A68AA15
          "iutQ":
"E02ECB188491AA1CC0F1DB49791D2819A9763253F9C657FB4A8E9808C6747073540FD4CF7354DDFB58C26561
          "iutDmp1":
"16E1B6FDFF69205A16808A58B553F1ECF0264082C5BB82B14BE46E8A7E411DFE71E3B62B61A074D229237261
          "iutDmq1":
"D11E14BFDF3E933A93C52B3772E5716FB482640936DD894621152D96A86ABEA75E0FDC5779F9310644F9DD09
          "iutIqmp":
"3EBA80870CEA803D15D0E7F51A0F2635D87FB8BC9A09E20925DB444153DAE45B3787042693CFEAC1541D56F1
```

```
        "serverC":
"41A97A3CB441792D7B6D576FE5CC6FB4CFEE4BDE276070E76B7C4E10036472B0D1C9C086FB20C8101E144632
        "hashZ":
"02B5979294F51A0802DD69CC52F6F29C1223FDB81D471319D24B077BDABFA60E0670531E792C7D3EC25A0212
      },
      {
        "tcId": 24,
        "iutN":
"B02D9D7E57553A8E45BC0C13BE37B3C7A8C816F37B016609236301BDD8F901044BCDB2AC3C0BB64272CC0728
        "iutE": "0CC25DFD",
        "iutP":
"CADAA00A7CF7DF501A5A4BB82D61909FAD3E8DF95C07C6155B7CD3EA1A17FD703EDE2413587F55D9F20DAC14
        "iutQ":
"DE55D935FFA0422E7E51C27A06730A80DF1F207DC48FC5A0C40DDC61E047660560A8DB60FFBE914CF1CB5F20
        "iutDmp1":
"C5EC3938AD2351E43FEB52075A1EF4A4EFF532F2EC1675C9818A51FFE878E7062510AA1B2CD6E561222B5573
        "iutDmq1":
"561E157985DF35BDAA1084B231137B6CE9F94CAB1909602A164E6E4C2E9AE209BF9F00F407B1A80BB24C7084
        "iutIqmp":
"013E24238C37B0560639D5F538D8E526E88A7D1194E83FDCD8FEAD609111115D6A6D9D56535E92AEC5EEE652
        "serverC":
"448EDE14B1D85F240484A3F84FCB67BF9630283B1D6CD13CF01FF9D56239BAC5EDC11C719A0EA527B9F9483D
        "hashZ":
"E589E60545994004ECE1CD9381634F68C38B5C63FFA9530237ACFCB17F04EB1B1487816F173525B851625413
      },
      {
        "tcId": 25,
        "iutN":
"8A04FF2183788114143725464BF867B9EA3E90046EF3AA5844CAFA0D39BEA3EB1A2DE3C0D513AE97F9022000
        "iutE": "037AEAB7B8BF",
        "iutP":
"B9AE73F5B6B45EA52AF4FB8C2EBD38B14088CEAD8A3F4694891C7C82AE330DAC4D232437D44013A4D3A2E2D6
        "iutQ":
"BE49C9BBA74514665F638E70DC04876636DF226D9C033C281D1E37503C87EE2166D0477FB1B5E25F069C9DA7
        "iutDmp1":
"2F172243E02F45A4909EB6EFE50BC84231A24D6B7022E7F6A6A5EF917493F21B8B8B0BC16EA0DAA050D28033
        "iutDmq1":
"507045A77827305B73CC02D38045C64CBEB67FE5F32D0F26234051DE452F413E095CFC0AA6CBE663EF147A46
        "iutIqmp":
"5CF90AEA702500B8A2CF65EB6A8BB36568A2280B924A15C591F034BD92D8176B2C56ABEDD77274C49D9C718B
        "serverC":
"6E16762F1E2DFB14E7AB9963DE9E1A153B4E5E11F31ACB323410385D6996FE8F012414B10C03320279BC1369
        "hashZ":
"CA2E91C53CD8381F49EF051B3353297FD5581646403833FA84DDE47EBE083668624F2EBAFB041B73579E1D2F
      }
    ],
```

```
      "scheme": "KAS1",
      "kasRole": "responder",
      "keyGenerationMethod": "rsakpg2-crt",
      "modulo": 2048
    },
    {
      "tgId": 6,
      "testType": "VAL",
      "tests": [
        {
          "tcId": 26,
          "serverN":
"DF44D1628F68B416721BF22EB07BD5815ABF0607E6055B6220E0D4253E82C65D4CD65907529B6018FFEA225F
          "serverE": "0D40123AFAD7",
          "iutC":
"3E2D993E43C72DE754FFC3F950711172B6C666BBDEB6F1C2E7F983C000307EA5C24C5BB91DAE49AF45FD24F4
          "hashZ":
"E44C582E69A52FE636F71F82E4851C4429FDC1FB98FC7D72713C1B62761E5E63D14D20DF6F827C52F53A15F2
        },
        {
          "tcId": 27,
          "serverN":
"B56ACE1CC37BC9AA5ABBA541432FE5A0DB6F8527C2FDC6BE5E4821FC46286C8C96F1EC19AE382188E49C95CE
          "serverE": "32F57FEBB292F3",
          "iutC":
"14E3F0C4005E7E91A09C9F3F1663C14215B147D509AFABF5B7D97DEE4FCF783749FE52734FDF9B2CDAD88D55
          "hashZ":
"9B70A3525F21C143AD49DC2E19F3B1D735C56E98731944382052AECED72F7C289C4AD41DBB8058FAC3160770
        },
        {
          "tcId": 28,
          "serverN":
"A3608F8BAF05F8D1E8947D546577620D68A3311F7C5121943CEF973588D8B3525EBE5BAD978EA3DEFBE0F324
          "serverE": "2F6D5E21C3",
          "iutC":
"70C43B6BCF8FCCB3563B3980EF6911E229C7559822CB17DE4288CC0EB38E403D5CB9246BAD2674134542EE64
          "hashZ":
"C2AED5B7988B73ADC59D31C1F92E3ACF41264BB712F5B75F6AD18FFD1D0DBEC6E201DB5912DD5C8589A62B0E
        },
        {
          "tcId": 29,
          "serverN":
"92DA7E667CC0022F55346B33FA14A254ED163B21174FD30501CB7466A3E4F921842BDD40D0A7FFACD311CA7E
          "serverE": "0576A52493CF",
          "iutC":
"6E2200569CBA3EBBC93505C58D3F391F4DD3B178750ED15892036D260881CC26AE59193960CB616618387BFE
```

```
          "hashZ":
"C9A42F617E8C11890D545C85514A07F84ABB667B526A850E32FF977B18CF16FC9FAF36721ED176FE42DCDE28
        },
        {
          "tcId": 30,
          "serverN":
"BFD0F63834F3F3D5CA4B5DDAAF013E995C259B0AC2894EAC4639FFB54B78B353BF64DF367A6197A3EF78C90F
          "serverE": "3B3D85F06107",
          "iutC":
"9548D09AE2A67020E08CC1887DD4B1940EEC3345BA952DFF31ABCE63CF87334EFA11BC1FC41833610FA4B6B9
          "hashZ":
"E0C0135614065FA78B7DCD3047B51E8A40203F7576997EA95BDE579938226E75F305D212097BE8B99802ABC9
        }
      ],
      "scheme": "KAS1",
      "kasRole": "initiator",
      "keyGenerationMethod": "rsakpg2-basic",
      "modulo": 2048
    },
    {
      "tgId": 7,
      "testType": "VAL",
      "tests": [
        {
          "tcId": 31,
          "serverN":
"9192857447D457406C3DD91EAC7ECBBC5BE841FE01C2482AF20CF1EDB9BBC6E9600C45400257E064AB9558EE
          "serverE": "0236DF2E7311",
          "serverP":
"B667988C421069B880A99FA6ACC9DEF8494C56E9C6F7BFC4EFD01D64B5A01BC949DCFD57670BCDD5E02005BA
          "serverQ":
"CC4E8CCED7A95BEF9B05C469E129C15F92096A700248494CCEF843DE7235099BC3A7BC9350A7B5FA17AE32F5
          "iutN":
"C35967858F2A658C9671DEF545F218B7A9154A860B8C3BBD403E509BD8F188C5799EA479372036E0854C8337
          "iutE": "01BDAA3D1EBD",
          "iutP":
"D23052F059494C8ABF2A10DA300FB024557E0E74FF380F7873BABFAA83A6693EBCB4C6D368744481062D348C
          "iutQ":
"EDED185C3DEFF77EA81D733BB27820AD9E1C70DF713F523B248D2BAEACF396864E9A3378E83CB7483C0B718B
          "iutDmp1":
"C84978AB90A0124A8C7B6B26408655FC4C6F95F328BC87002012DAB8AB05FAE45DDC97577AF7FED742AAE980
          "iutDmq1":
"C3354F4569307231DE1874EAC9E28659DE6D2A10A4D5204E333BF202D211C25451E0489274B5131ECE5E7A53
          "iutIqmp":
"6462D3FB8531E46C1EFDFEE16856F30D62D4016CC8E7700441E1385929DFD9D5E1158F6F55093892B6A7303E
```

```
        "iutC":
"8E5EEA2C097D2BCB44E53CC851BAD6BC71458C571387AAF339CF888B86AA1EFD4026580B21FA23D45E7BE5C3
        "serverC":
"BA998183F0AC88955E598F39856E0AD4B2A7DF9CD314FF46F4E8B0FA660DBF8E008EEEA7ABC3743F286C46D6
        "hashZ":
"8741D13ECB37752B1B15DDBA8368A0BD18497B56183E90703FCC660A13A7A8ED8C933943DDD33777866FA16A
      },
      {
        "tcId": 32,
        "serverN":
"994AE3220AAF55C797BE23ED82C6CEB2F8008132D1ECDC8A580D70A9EC1B9248A0788D3E6A988E548F7BBDEA
        "serverE": "3D0CAAD6D81F",
        "serverP":
"D2551B98F4BC1FCB8E3A2A54E121E1DFD91C075C17690A906A6A7E2482398A1B3B2B69B23D3010D7F2319F48
        "serverQ":
"BA9355749AF431217087F8BC188E9732EED5044F7FF292587DE5EE9EC2125018B9B17CF31F44497D356DA831
        "iutN":
"ADF15717BE3EC9BC288258DD92C738C16021B910D557AF3C270518CD45FE5E16F4BC8499DC5AB39D7D74F539
        "iutE": "F308BB61",
        "iutP":
"DC3759B59FA2577BA58002FF7FAC7CF4FE974860EFE75B941DE2544F584822A6986AC8D4751412E15D8B74AA
        "iutQ":
"CA3515E8DE397A64B893928EC56E2A604684BDC09B74D6C31700144F344B0BF797DF5434A718EACB26BD8E23
        "iutDmp1":
"7B3D8504B3CA6690D5B00715863EFCB0D5E5D410A8E90E7C41C0985C233FCE59AE586DE8C4A47B73A8889278
        "iutDmq1":
"1D97F76C72201D006FD1D9570215B178C5FB222E65FD0AC35408570FBF907EC18543A430D2409BE95A44B8FC
        "iutIqmp":
"6CA653698B01E880FCFC3C85FB2DA1F5418241DF1BDB1B439520A8C6C59C35AC36BB53B79C2114337CCA06DA
        "iutC":
"4BC29C92C3E2E5DE79593BCA04E9C9DEC9EB968497238EE3C3410FCDBB8240284724E861E27103B71130C800
        "serverC":
"4A1F96BED48531F09099F7D47E893B849CA4982146FE2B8F76EE9E607D5360D06061C07F95E2E72CD8DDD09D
        "hashZ":
"CE3CA459D4409BE1EBF5708361EFFC3FC56A475166A5A8B55436654AB6DBDAE1E29EC662E9415B78FECF5DF7
      },
      {
        "tcId": 33,
        "serverN":
"AB91152596AFD57607949CB097A64F3E084F9E99E09A83B56692C2B6A28B5C567F4CCE72527411CD154F0AEF
        "serverE": "6DB45311C3",
        "serverP":
"C80FA01543FA4BEC2E3B654FB83802A62FDD3363BA1000009BD1206F352F19983254D26B873D6B48DF462E2F
        "serverQ":
"DB89D57D0D37E538E346B86FA599684EC0F2289A0E69D703E74D0DE58460865A9F6F6C76392771A020366156
```

```
          "iutN":
"D7C77D9CE72B22B232432C9D699950F71D9579B8CFA882032432B36D711755B3D436E3F72C0A4C8A296EB1BB
          "iutE": "01E5FEA52FB4C9",
          "iutP":
"E894AB6D65547BF1365A7144A52CD16E4B05652E741C1E4FE20C069491BA90092EFDFD8F9EABFD08E5F85830
          "iutQ":
"ED81B8E8AC06979E225FECB0171C835349E290C53D2976E94DD66855528E4A4C8935A8C88790194F8AD57D46
          "iutDmp1":
"CFBC119F2834AEBF8B566EC59376F76F069C5662C0A54B4DF2405CDDB3EEC4760682579F80AD99F08C65CDE7
          "iutDmq1":
"2CE92A623EAF4EED50873630799A02C3D9EC04C87AEF30794FB3DA4E145112C1E9B661337BD16DB074FFB871
          "iutIqmp":
"6A33DFC5E347DBFF96989D29F638DC4B7E153D057AA76AC77263148F01B3912017498F26FDB304D9453DA881
          "iutC":
"14A4EB220ADA378590438F1094FEA28A2BF6075D228FCFF75D465EE6364A3A818552D9E7685E5DC6295A9337
          "serverC":
"7CE9122C2C9FCC6CAC8453A4D16F09A798E782E4620F1C10AD655AC842EC250BC6542C16113BEF57787661E2
          "hashZ":
"40E9FF55661B9C5067412F06E90018DA1D32BC641D523C30BDC5C20F508B3E336CB0DF03BCBF1EB22CFAB2E4
        },
        {
          "tcId": 34,
          "serverN":
"8BC2AEB4A7C2FFC5201CF8AC163ED580BD914722ADD733BAFC57EE5A45EE030901AF1D703ACA46457ADF99B9
          "serverE": "C0651DC462DD2B",
          "serverP":
"C513607803B7DF7D75896E18DCF2A0A8EF5EC78A0111BD241DE59580D2EEB811BC2B60133D2F00C8D2AD11D5
          "serverQ":
"B58C44B853117D3523D5A9B1AD321BF5EE78970EF09EC1E49BDD7353048A29C6A8D96AD2D7A1B8FC46909534
          "iutN":
"C6831B5E10016C30E798B70A3F99F1BE73217438CABBD7FE4C504371FD0017A020101708A6765D4E27F0ADA3
          "iutE": "3FB5C2C01C8D",
          "iutP":
"E2DB4709A26FE8B9D785EC1D72871E657B1F9C9C70CD55FCE6B77ADD65B5B83F161E57E73D7C7C7D5A7C15C1
          "iutQ":
"E003A7BC2D9360D3A77085B8A91E8C1670B7E58D86BCC1C9C467105DE02B47B926228D332AA33CA691695C3E
          "iutDmp1":
"DCA1A93C6C60A48F5BE6D6BC4A4201657585A0FE1BC47BA010DDB687840B1B906925F529DA45BB1602CFBE92
          "iutDmq1":
"639503AC9E8A79EA5BFB7CC12F7733A4ACD6E0BC85ACDED3BAD57C804C23F041C8A51A976BB3E65C648F22D4
          "iutIqmp":
"C3D37D174E95466681AC31D7A80DA0A404BF0C0151428BFC193DB750A528AC6E35E281FA93E8F3B61523E960
          "iutC":
"7CFE773662C96CDC81ADBC12B11A31CC2EB8E349F39F93B7B756526685208F7657C7B30E6F565F9739D86997
          "serverC":
"230286251C713042DE65339BBBA956F197E1FF490096F4CAC58BC1211608853980116C26CB15AA687A947A3E
```

```
        "hashZ":
"C620B4AE455B12F1A6278FB6F6D754B5155CC1E74FCB270A0E77A2C81327861F717A9C1494E44855C7039D0D
      },
      {
        "tcId": 35,
        "serverN":
"D4424D3075303354B0D993FC058FB4B9E07F88D5C8E28BD9E0FB8FC6076001837940A27449E8F6387C129438
        "serverE": "8BBFE1B5",
        "serverP":
"D66C5B6B2494DDC1525D74EBC74624BA5F312E0C0CB0384F96F0FAF8FAADC4FF8A144DF5CFCC6EFCC62A2966
        "serverQ":
"FD6A834CBB1C6E49F745313EE95C2189093FA0D5BCA8EAE6954390781A159A48D2C6674D80ED5516B2FB5A3B
        "iutN":
"B0F7E76B3890B95C65F8881A2BFA539781379EEF0E31AE8999308F9B2D283F1F13334BBE5A0D40AB4E5491E5
        "iutE": "C0A50FF6E3",
        "iutP":
"D0996867A4E8D74785A65D15F75D3590F4DB7EF70FAACD41E450317BD3810B1DCD34FBA0D211DCC18B7007B3
        "iutQ":
"D92E78B407CB267CAF20B2B4A50CF7A859BDE11F2025958E899EB2A523FACDC4738680F4353EF5EAA5F07897
        "iutDmp1":
"5D2DE6806B87D29217DDE89F48606041D04558E3DD2B2D4722821B2A0522D0873141628FE49D276FD4C01494
        "iutDmq1":
"AF62AA2CE393F57D348881F8F6A007B077FBBC82C6685BE588BCF8BF5529153B052E6110760448B05E323A11
        "iutIqmp":
"4FFCAB492D6925A0427FACD027BB00863C4EB2BA0BA9D184D90F1D0ECC403D12DCBB0801B8CBBCA519C04D37
        "iutC":
"631FA888F909B577175BD5F94A4C09D6401856F8BA82001873F4C7D3CCD27824776829CF1C226455BEF54819
        "serverC":
"6194F739F5123D74262AE8DDC70AF5C0B0178D13B633FED5DB1B005357361E2250B041887DD204F3E60FC5DF
        "hashZ":
"00E7C9AA3C9DB0354A4ED00F077E7EEC9FF4B45913FE5505C110CC457277499359547F3CC33184E28C250E1F
      }
    ],
    "scheme": "KAS2",
    "kasRole": "responder",
    "keyGenerationMethod": "rsakpg2-crt",
    "modulo": 2048
  },
  {
    "tgId": 8,
    "testType": "VAL",
    "tests": [
      {
        "tcId": 36,
        "serverN":
"8F7BD58C07D1F27432433A3A5CE8B3F9C03FDDBC4D666D060242AA0DBC37A6C1CFC143D3F663AE348251F929
```

```
          "serverE": "1730DA1731",
          "iutN":
"AF847417E711C3D06C70A43CBCA543F43707C27D4E2146A0745950B6D6E65AD7A796EE9C932653B7E19FD1FC
          "iutE": "019EFAC9F7",
          "iutP":
"D3DC54C574AD9B9CDE1666B26A8F6A5F8A5D0AF2F77B2F924FF9EA903B329FC30EE6585134319522D917200E
          "iutQ":
"D415BD7D61F8A3D520E01B68BD2BB6D142EE4D4B58283B009CC525EAFA9F45828E0E22B4DB218271F9D50B3C
          "iutD":
"33D46643F364BFD0F0B8E6BD0B7B2AC57CE89AAE9B2AEDB06D8A56F5133A786DFE5B9A542BA5168C834AC1EC
          "iutC":
"308A907845173A7C76D7C24172453CDBFEDBAB0E9055C973E658F4BC98D3B3820C96F355DB586B1A09A67FDF
          "serverC":
"502A1ED0DFFB16331081B7CCD6790E0F58D859FE34EA901073AC15D88E8D867DB8B145DF08B29EE893590361
          "hashZ":
"B17851DD72D1D071A1558D8E63F4A7AE2554E47386FA6DD626407F077A4F0817D842F09E86A8CAFE4BC5DFE0
        },
        {
          "tcId": 37,
          "serverN":
"CCBA31A69EB3A427285DE2776F4141EC487DEC8654328EE9070AC776045DFD25D5D8ED64B34E272EA57104C3
          "serverE": "27C59C91A38F",
          "iutN":
"ABD12FA689893CBF98DACC28CB724ECE0FC33B872F979D4AAC4C9CC46BFFFC018B3900FD5A88FF64C65E4604
          "iutE": "A6C298414925",
          "iutP":
"E70219659EEB84AC605600793C13D045E425EDE6F58E21048A78886375E945BEFC31F44D2EE09EF04D8CECC0
          "iutQ":
"BE67C1E26B29A76332F4970B24F0209B3C044E344A24E6F97D5A17E363C44FA3CF03F76F80E706E51034D22F
          "iutD":
"0292DF84AFF28D4D25BB6326499B8E53035AE958E4CBE1FBA7B1F3CF4955964E66880B94D7B4493C67C29EE6
          "iutC":
"A9B057F091FA424440601F2A138897040A7F41444C2130B273DAE163BAADD9779B71D4F8BEF23FA1CBD6C9D2
          "serverC":
"AB77F67FC4E81DE1324C6B8A1F3D0CD5DA362736F00D8F79751F946B952EBBD02C2BB9D841FB347520063039
          "hashZ":
"2E76D32DB11C2A0DC01724DAFE4D0C821F828E28CD8C7A63D4A63032DE840FA876E204933D4F6C158A4CE48F
        },
        {
          "tcId": 38,
          "serverN":
"DCD692B0F9AA9B9383E21BB48E56659D067FED89FBFBDEA9CDFDF0B8381EA4D9A60D54B3FDEC323725B1FB6B
          "serverE": "0FAB87A01B",
          "iutN":
"C45C4945AA3CB2AA190DBD21142C309A4F2F9169183C56A3990F1D15D10FA444FF4AD762CF024C682B01F590
          "iutE": "064E338E2FF913",
```

```
          "iutP":
"CB9E85E87038BFE35729F5A0AEE118B0AD721C944EF44F1BD42F2E6253501483A151BA6E36ED906578A16369
          "iutQ":
"F6DFBBF781B1F34C26DC3D8E4F14D3B0231668C6F6E411D5D0B5041C37C2CBA5BB234DDF99DD353B64ED8679
          "iutD":
"5BCDBDA12789253101615DC0985DF0618D2856BE339E317C74B7C30E77A3EE3FA178CF80DEA836955CB54842
          "iutC":
"A32D353D4484576E9DE9245FBE09C2F97C7E2F0CE12A4F15E48AAAA9A6A0642D2C353B0FCDC49C5B45BB9C12
          "serverC":
"A6FF08E60F38356D3DBA280CD803E5ACEC37ADC9202BF5FF3EEA660503DD22D9CC49F2395CB7B9BA7AC28DD6
          "hashZ":
"8FE0B23EC65E2EFCD879EADF4B15197228AB67B04103562EB09C0B04412EBA142BC39714A975202B836DF65A
        },
        {
          "tcId": 39,
          "serverN":
"B9A0D1B88CDDFF47D78E1D799E79B17E063261CE8E394B879421746AD613751D75300B1E99ACDC23BF5FC582
          "serverE": "C5EBCBC5",
          "iutN":
"C0C9BC1131F43B35AF2693579EDF360B5FDD90E8C5E76D53B6A50259CEFCBF0D1547096AE26F8A55E0F159A4
          "iutE": "966456F541",
          "iutP":
"CF516B9F15FFAD9B95BE52B3BE944FE53CF3F0EFB2EF697CF3B4B94191B2E41E2E611D0EACF9E8BE5F71C7D7
          "iutQ":
"EE0EDDB95F2648AA6C42A3E9122F9E8A04C503A13858933F70F6285D90234FE6CDBBE6253C09C91FBF4688A0
          "iutD":
"C0B3E46E9475970FB83A12F26847997A51DD6C177A031905852029F6B16002022CFE3139C06901FAA188FF6B
          "iutC":
"147ECC911BA999FAFFE8880F192C88829575E1B9797D3FF4EE793DAD14FD07DC3F9C1ADC694C4AE3404753B6
          "serverC":
"3CB801A6CC7F07CD9AE92FFAF3924132074EC0EF65E7BE9938B168DA6AD6105CFFCE8F70EB0E8AEBBC0A5E27
          "hashZ":
"08468B2ABBFC239EDFDBB8662CBDD3A6E0A796F74F4DFF525C7966529D2C0943D4A0E483484CD5C56D4AD7A4
        },
        {
          "tcId": 40,
          "serverN":
"D3DA155FAD198CA97BD2AE1DF1DAB5DD74FB8A75E8C4700A169165D1838F25F55EA51E4F7E428529B7A1B7B0
          "serverE": "FEF013683ADD35",
          "iutN":
"A7BE21FFEF7B27A3306A5FF03A60D3EF30B868EA2252205FF6A66C6D0F98C8B5508A25AB1CD65ED2F9D9C37A
          "iutE": "0EEF9110F795",
          "iutP":
"B53E2588AC39C8CA8ACB7C1EC5776EE937A7D9B258600017A918A842887A1D127AB4B2B83CB7D6D61C73D6AF
          "iutQ":
"ECEE7BC32F0024D111014258B94E5F95DEAEE502B2DB3353A76418DE11152367611AFF5C671F6132B03D01A3
```

```
          "iutD":
 "36FC5588780D0A02FB06EEAF349D0CD3ED1CA5AE7368152F673F17D75468D9577E791C1E94CE8EA351A40282
          "iutC":
 "39CDA01F3CD2664930CD634CCDDD284A4A09785C9BF14A92AABFDEA49046B089B4B6433A54420BD62EAC9BFE
          "serverC":
 "58AA75A09D7F391932A94E974A7A5C55B91A8F3537DBD4974CCA1D719A5CEB5F395EE89A3E421E9D01648FAF
          "hashZ":
 "3D7B6FAB0D642E2FF535F3A506AC9A6F43BABF01A223BF7C29FB6385D11DAE8E33BA0E46A7265D528F8E48A9
        }
      ],
      "scheme": "KAS2",
      "kasRole": "initiator",
      "keyGenerationMethod": "rsakpg2-basic",
      "modulo": 2048
    }
  ]
}
```


**Figure 4**

# 7. Test Vector Responses

After the ACVP client downloads and processes a vector set, it **MUST** send the response vectors back to the ACVP server. The following table describes the JSON object that represents a vector set response.

**Table 10 — Vector Set Response JSON Object**

| JSON Value | Description | JSON type | Optional |
|---|---|---|---|
| acvVersion | Protocol version identifier | value | No |
| vsId | Unique numeric identifier for the vector set | value | No |
| testGroups | Array of JSON objects that represent each test vector group. See Table 11. | array | No |

The testGroups section is used to organize the ACVP client response in a similar manner to how it receives vectors. Several algorithms **SHALL** require the client to send back group level properties in their response. This structure helps accommodate that.

**Table 11 — Vector Set Group Response JSON Object**

| JSON Value | Description | JSON type | Optional |
|---|---|---|---|
| tgId | The test group Id | value | No |
| tests | Array of JSON objects that represent each test vector group. See Table 12. | array | No |

The testCase section is used to organize the ACVP client response in a similar manner to how it receives vectors. Several algorithms **SHALL** require the client to send back group level properties in their response. This structure helps accommodate that.

**Table 12 — Vector Set Test Case Response JSON Object**

| JSON Value | Description | JSON type | Optional |
|---|---|---|---|
| tcId | The test case Id | value | No |
| testPassed | Used in VAL test types, should the computation of a shared secret $z$ been successful? | boolean | Yes |
| iutC | The ciphertext computed by the IUT (using the ACVP server's public key). | value | Yes |
| | shared secret $z$. | value | Yes |

| JSON Value | Description | JSON type | Optional |
|---|---|---|---|
| hashZ | The hash of the shared secret $z$ for instances in which a hashFunctionZ is registered. | value | Yes |

### 7.1. Example Test Results JSON Object

The following is an example JSON object for KAS-IFC test results sent from the crypto module to the ACVP server.


```
{
  "vsId": 0,
  "algorithm": "KAS-IFC-SSC",
  "mode": "",
  "revision": "Sp800-56Br2",
  "isSample": true,
  "testGroups": [
    {
      "tgId": 1,
      "tests": [
        {
          "tcId": 1,
          "iutC":
"BC52DE87B867C97ECA449712EEB9BDA2E806EF230FFDA78B2ADF09E75B1276D9243DDDB9C78C88D2E9F6DA70
          "hashZ":
"B48A0B2BADAC02C8018A8E6DCF5E3B999C816F137F8475F700B2951252968A272B738052BDBBF759B6DE7E25
        },
        {
          "tcId": 2,
          "iutC":
"3E84C8478A7EAF1E20A360427E8EC57CA81772AEC5153FF7348F38510366F7A07D1A09CFC49DB7F4BD4B1858
          "hashZ":
"473BC4F1CD3B42D4F2A77F54208CE3B9D6254E82D2AC68C806FD9219FFCA97CF1F8C8D0CB446AF6FBA1CAC06
        },
        {
          "tcId": 3,
          "iutC":
"9AEB3DD05F2A71018A7E25F14FF577F1E31538553C49A6EAC534CE835FCFCD4719937026C46F58ABA0F6A6E1
          "hashZ":
"8EE8AD2476627C57C0D994C14C5B11007B598D7FE9121970C507DBBA0C5F2555D49DB5FBB34802242DDF978B
        },
        {
          "tcId": 4,
          "iutC":
"56C9CDE42CD0792C043586456561AD2C2FA3224714DCB1A5DD80677B606890AD9DB7BF4D488FE19D1984A398
```

```
          "hashZ":
"96ED3D03DEA33E2BEAE8835CE7758308F035D28CEF2F9CEFF474FE8156878B516C045F345576DEE53F7582CA
        },
        {
          "tcId": 5,
          "iutC":
"26F490F8AEAADF2C39580CEDA771163FAD23476B1E33CE900DCB738E1C73DF38EF439A7D72E751A058FDA842
          "hashZ":
"BB0FCF7CDDBAC2A38DF7A7DDFD76324B5A8C4208846EFE50E5D2DC21472FD3D053D88A58979C4519EF58A2A5
        }
      ]
    },
    {
      "tgId": 2,
      "tests": [
        {
          "tcId": 6,
          "hashZ":
"72873353BA81E9E3F97C169180850C6A342FB70258AAE0CB9217CAE2736FCE48D66295BB776EF518A97A8649
        },
        {
          "tcId": 7,
          "hashZ":
"66456CCB689956E171E7BBA83FA7659A2DD313FEBD915F74D392195EF48DD250C702FB2004DAC9D2AAF787BA
        },
        {
          "tcId": 8,
          "hashZ":
"A62646DD4C19E41476E1FEC16CDAE7B9482EF54505A1FD111DBF4901D0D7E590B949B00C437A642F3BD8EF6C
        },
        {
          "tcId": 9,
          "hashZ":
"25053C4FFEBB4D5553E7AD9A8097A8A8BC17B2CFDF25F71888DAE69F77ABEDDFC01BF064E90D839B20BEF4DC
        },
        {
          "tcId": 10,
          "hashZ":
"F2369C65E6DEDFC2CEDFEC8DB2CE06488F6341B34E64941ED1A26276C4709526D758C8844733566D32711D8C
        }
      ]
    },
    {
      "tgId": 3,
      "tests": [
        {
```

```
        "tcId": 11,
        "iutC":
"7165F43606D75D9E0062C23BDAD81054AF1F5DD867E6DF01C63D91F172EAE9857570315DE6CA985C612624B5
        "hashZ":
"9DB8AE3B99C33BE2717443F204BB96A850212615310B035AC327F42558F37938244621FF4D9D3B95C8874B40
      },
      {
        "tcId": 12,
        "iutC":
"7717EDC81D539C9E75C679C7C7F25E4BD0FE88D1D0E8A1DD61E4FE35C34E7293D80A746102D1F250C8F4EE78
        "hashZ":
"280EDA51AA55D0CAB3D61251B0BE8AB1D9B89ADC8D0C53FEB1B3CC33A7662BF72F648F941AE8D6BD35DE143C
      },
      {
        "tcId": 13,
        "iutC":
"15334D04B783615DCD85751A26DC7CA999F748A21C524517A4E8AED82EAAC56205951388871F22178B278AF8
        "hashZ":
"DF71B0DB82C2E45F1B0DBDCCDA7A00995FAC3323008FC89775DD93A2BEE553F9B0558264876B05EB48E11B71
      },
      {
        "tcId": 14,
        "iutC":
"46BF8D84185254F526CA1BACB8EE2805245841D54E7434CE1CB3D578B1BAAC74273B46464233430F1CDCC1EA
        "hashZ":
"785E85B2F3693FDE598EBDA463D4A31BDCF6A8DD4122A1C625B361A6BA5654E322CEB863C3E6FB470687E143
      },
      {
        "tcId": 15,
        "iutC":
"97E01C6237F205CAE45CA143B872068B3E7CEC09F88277ED8253D336735B1E55D648F7F2E4C1EC5401B1B8EF
        "hashZ":
"B62B498E074E19911BF49D4C86DA2BC899550BFDC5880765F24ACB16731DB0F05AEC0563EB6D6F5B769368F9
      }
    ]
  },
  {
    "tgId": 4,
    "tests": [
      {
        "tcId": 16,
        "iutC":
"59918CE9E94E85F9B55761AEB56A9EC9316A4680F222014E61DE8E741F91927BAE90B598079D57620D018F6C
        "hashZ":
"5E925B5B8FBF09C85695B2DEE5F24C30AE5DD027A49A5DA3ACD880839D915BD0F591E56578598E947DF8F47F
      },
```

```
        {
          "tcId": 17,
          "iutC":
"2C1EF41FE21CD049F70E565FD1A583517DA56D8453EB49F7079DE5187F5991AE0A2E40CC5D66D532036908E2
          "hashZ":
"47D59912FCAC4E8DADD36631D30A37B33FF6EC033D71FAD6B81630B9A7FCAE22CD9EF627EC94683C577671D7
        },
        {
          "tcId": 18,
          "iutC":
"89B6E92E24812EE7E56E9DB0A710CCD12A92B2DCC30521980F87548E45A9F08A9A55E60B641394D7605180DD
          "hashZ":
"F37AE64EFC034F023335E05ED40D2578506AC97963A68E17D8964713A8D5339DBEC08A54271C72BA9B7966B3
        },
        {
          "tcId": 19,
          "iutC":
"AD8870E7FCE18E54127FD3C07B02D71BDD10E519C414320E1D8E61420BF1907990E7C12A9B6003B2E64F2A38
          "hashZ":
"0747F513741CE872489521180B33A569F60F3E3CBF8102A49EBECAA3AA309AD7B8463543ADB867BC80973C34
        },
        {
          "tcId": 20,
          "iutC":
"089EEE5C8B64FDEE6C4B79EE0CC903321A0B2F14CE3A89820E38FC2A34B666CE0A3B41C41E5F7E1975F47DBA
          "hashZ":
"1487575F667890C8693BC8A731F55590A5E94FA9171E1A324EAC37092B049E9FB7506B09D4790C7C3397BCC3
        }
      ]
    },
    {
      "tgId": 5,
      "tests": [
        {
          "tcId": 21,
          "testPassed": false
        },
        {
          "tcId": 22,
          "testPassed": true
        },
        {
          "tcId": 23,
          "testPassed": true
        },
        {
```

```
        "tcId": 24,
        "testPassed": true
      },
      {
        "tcId": 25,
        "testPassed": true
      }
    ]
  },
  {
    "tgId": 6,
    "tests": [
      {
        "tcId": 26,
        "testPassed": true
      },
      {
        "tcId": 27,
        "testPassed": true
      },
      {
        "tcId": 28,
        "testPassed": true
      },
      {
        "tcId": 29,
        "testPassed": false
      },
      {
        "tcId": 30,
        "testPassed": true
      }
    ]
  },
  {
    "tgId": 7,
    "tests": [
      {
        "tcId": 31,
        "testPassed": true
      },
      {
        "tcId": 32,
        "testPassed": true
      },
      {
```

```
          "tcId": 33,
          "testPassed": true
        },
        {
          "tcId": 34,
          "testPassed": false
        },
        {
          "tcId": 35,
          "testPassed": true
        }
      ]
    },
    {
      "tgId": 8,
      "tests": [
        {
          "tcId": 36,
          "testPassed": true
        },
        {
          "tcId": 37,
          "testPassed": true
        },
        {
          "tcId": 38,
          "testPassed": true
        },
        {
          "tcId": 39,
          "testPassed": false
        },
        {
          "tcId": 40,
          "testPassed": true
        }
      ]
    }
  ]
}
```


**Figure 5**

## 8. Security Considerations

There are no additional security considerations outside of those outlined in the ACVP document.

# Appendix A — Terminology

For the purposes of this document, the following terms and definitions apply.

### A.1.

**Prompt**
JSON sent from the server to the client describing the tests the client performs
**Registration**
The initial request from the client to the server describing the capabilities of one or several algorithm, mode and revision combinations
**Response**
JSON sent from the client to the server in response to the prompt
**Test Case**
An individual unit of work within a prompt or response
**Test Group**
A collection of test cases that share similar properties within a prompt or response
**Test Vector Set**
A collection of test groups under a specific algorithm, mode, and revision
**Validation**
JSON sent from the server to the client that specifies the correctness of the response

## Appendix B — Abbreviations and Acronyms

| | |
|---|---|
| ACVP | Automated Crypto Validation Protocol |
| JSON | Javascript Object Notation |

# Appendix C — Revision History

**Table C-1**

| Version | Release Date | Updates |
|---|---|---|
| 1 | 2020-08-19 | Initial Release |

## Appendix D — References

S. Bradner (March 1997) *Key words for use in RFCs to Indicate Requirement Levels* (Internet Engineering Task Force), BCP 14, March 1997. RFC 2119. RFC RFC2119. DOI 10.17487/RFC2119. https://www.rfc-editor.org/info/rfc2119.

T. Kivinen, M. Kojo (May 2003) *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)* (Internet Engineering Task Force), RFC 3526, May 2003. RFC 3526. RFC RFC3526. DOI 10.17487/RFC3526. https://www.rfc-editor.org/info/rfc3526.

D. Gillmor (August 2016) *Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)* (Internet Engineering Task Force), RFC 7919, August 2016. RFC 7919. RFC RFC7919. DOI 10.17487/RFC7919. https://www.rfc-editor.org/info/rfc7919.

P. Hoffman (December 2016) *The "xml2rfc" Version 3 Vocabulary* (Internet Engineering Task Force), RFC 7991, December 2016. RFC 7991. RFC RFC7991. DOI 10.17487/RFC7991. https://www.rfc-editor.org/info/rfc7991.

B. Leiba (May 2017) *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words* (Internet Engineering Task Force), BCP 14, May 2017. RFC 8174. RFC RFC8174. DOI 10.17487/RFC8174. https://www.rfc-editor.org/info/rfc8174.

Elaine B. Barker, Lily Chen, Allen Roginsky, Apostol Vassilev, Richard Davis, Scott Simon (March 2019) *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography* (Gaithersburg, MD), March 2019. SP 800-56B Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Br2.

Unresolved directive in src/kas/sp800-56br2/ssc/sections/98-references.adoc — include::../../common/common-sections/99-references-acvp.adoc[]