# ESV Server Architecture and Demo

## Entropy Source Validation Workshop
## 4/28/21
## Chris Celi (NIST)

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

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

# Outline

ESV Protocol

ESV Server Components

Entropy Assessment Tool

Demo

Client

# Protocol – Workflow

- Authenticate
- Register an entropy source with conditioning components
- Upload raw noise bits, restart bits and optionally conditioned bits
- Upload supporting documentation, such as the entropy assessment report
- Upload module metadata to ACVP
- Request certification, begins a manual review

# Protocol

- Based on ACVP, https://github.com/usnistgov/ESV-Server
- Two-Factor Authentication, mTLS and TOTP
- Mostly JSON communication, file uploads are multipart/form-data
- Send information to the server:
  - Details about the entropy source
  - Files containing bits from the entropy source
  - The Entropy Analysis Report (Supporting Documentation)
- Server will process and return the results from the Entropy Assessment Tool
- Submit for manual review

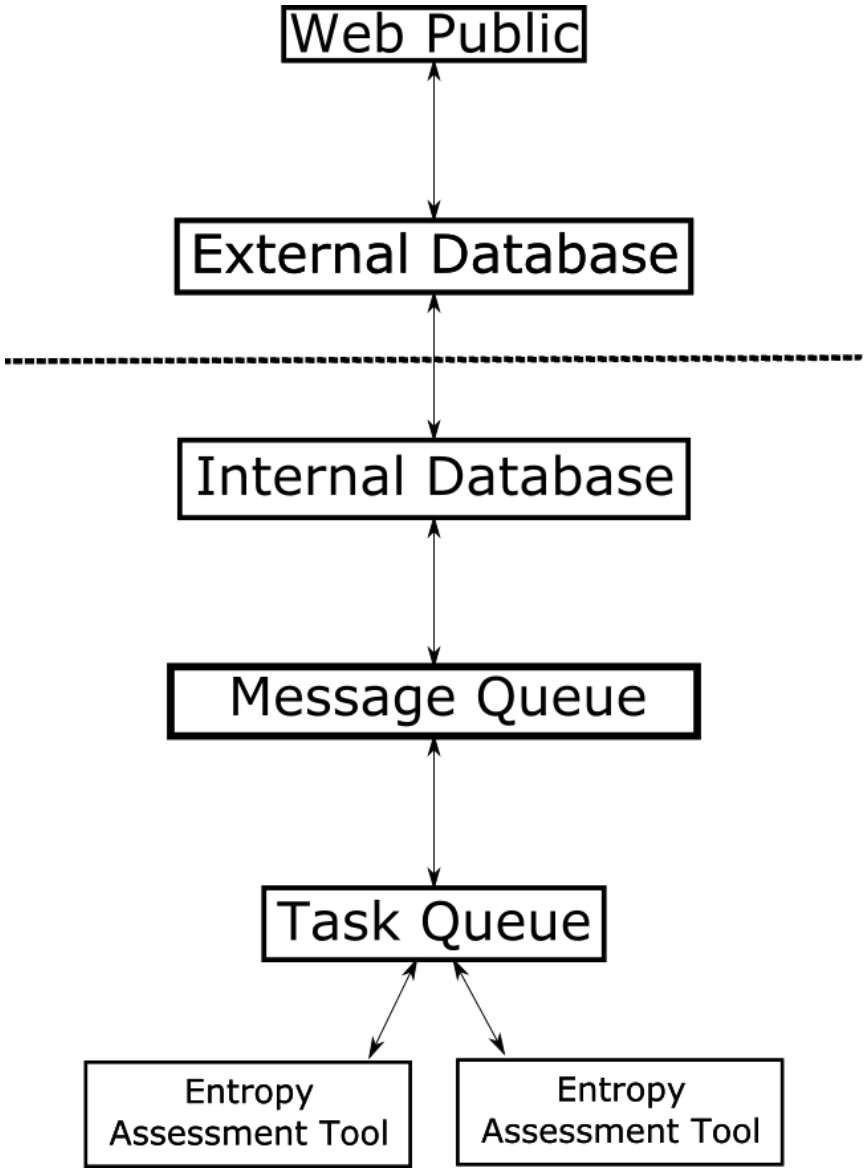
# Protocol – Lessons Learned

- Sharing infrastructure
- File uploads are always going to be larger than ACVP, and not natural to JSON
  - Includes .doc, .docx, .pdf files for example
- Certify is not tied to an individual test process
  - Previously unclear of behavior while validating multiple test sessions
- Lots of work upcoming regarding all CAVP/CMVP services

# Server Architecture - Basics

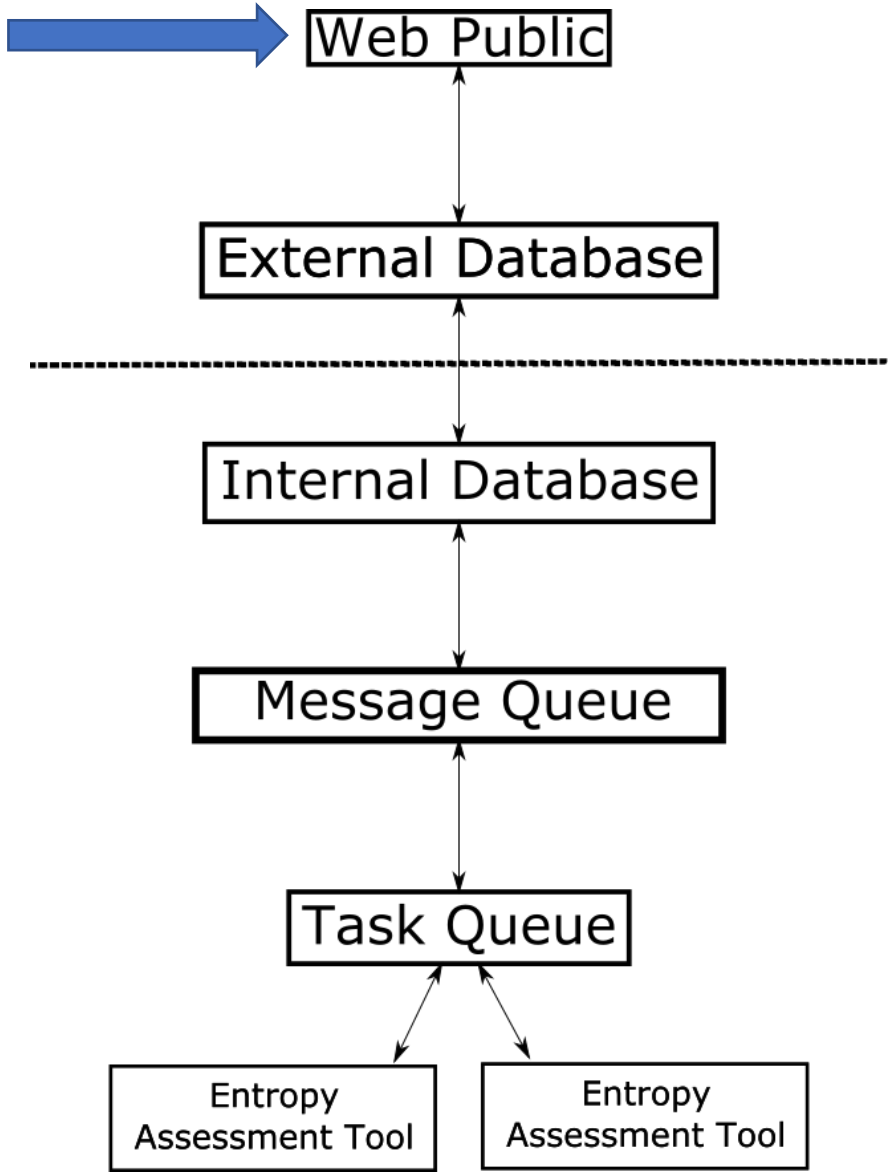
- Similar design to ACVTS
- C# using .NETCore framework
  - Updating to .NET5
- Development team: Sunil Bhaskarla, Andrew McCaffrey, Chris Celi
- System Administration: Bobby Staples, Jason Arnold
- NIST HTML Client: Janet Jing

# Server Architecture




1. Web Public
2. Message Queue
3. Task Queue
4. Entropy Assessment Tool

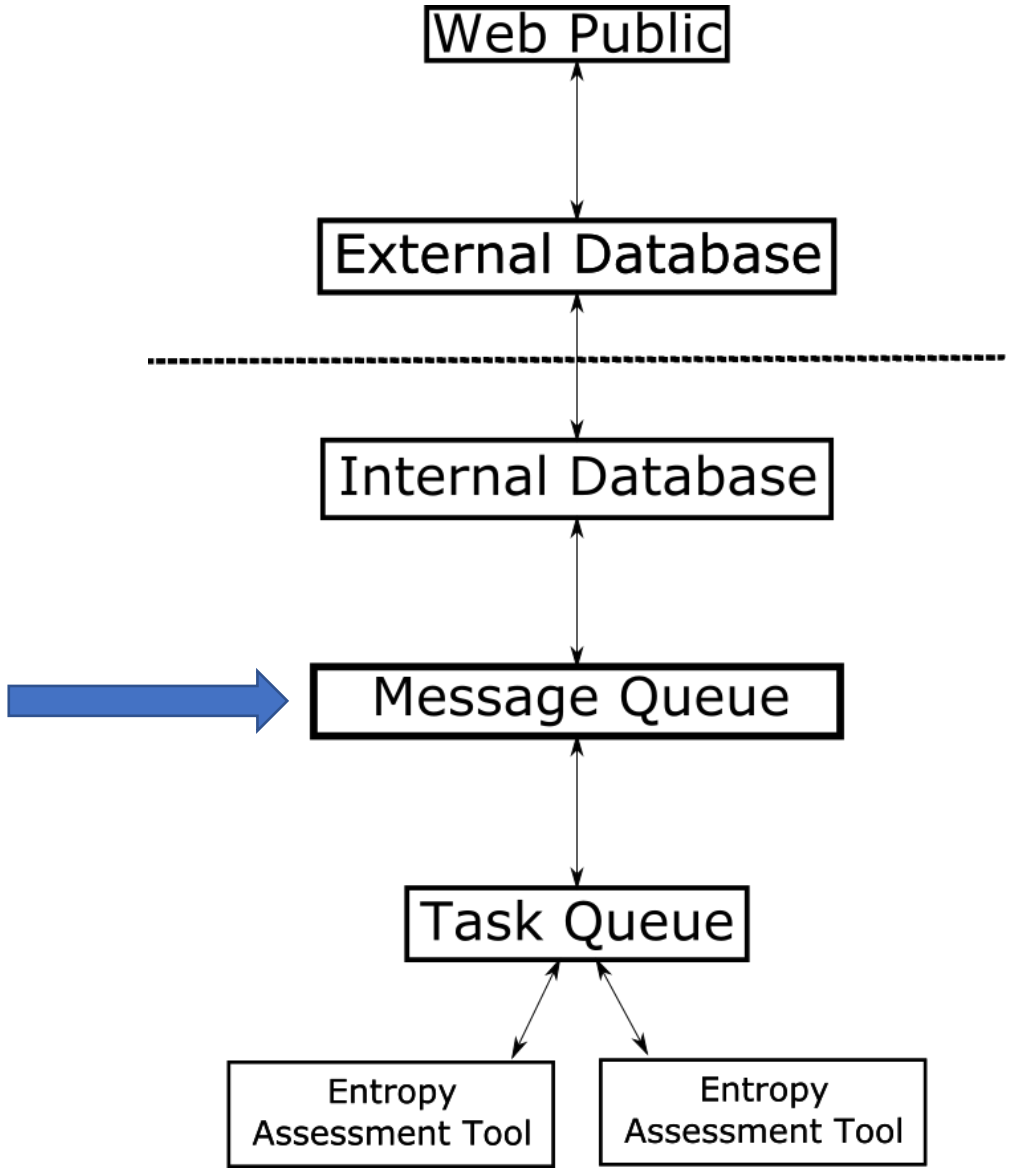
# Server Architecture – Web Public




- Provides JSON-based API
- Retrieves content
- Manages authentication
- Validates requests that are sent to Message Queue

- Identical role to ACVTS

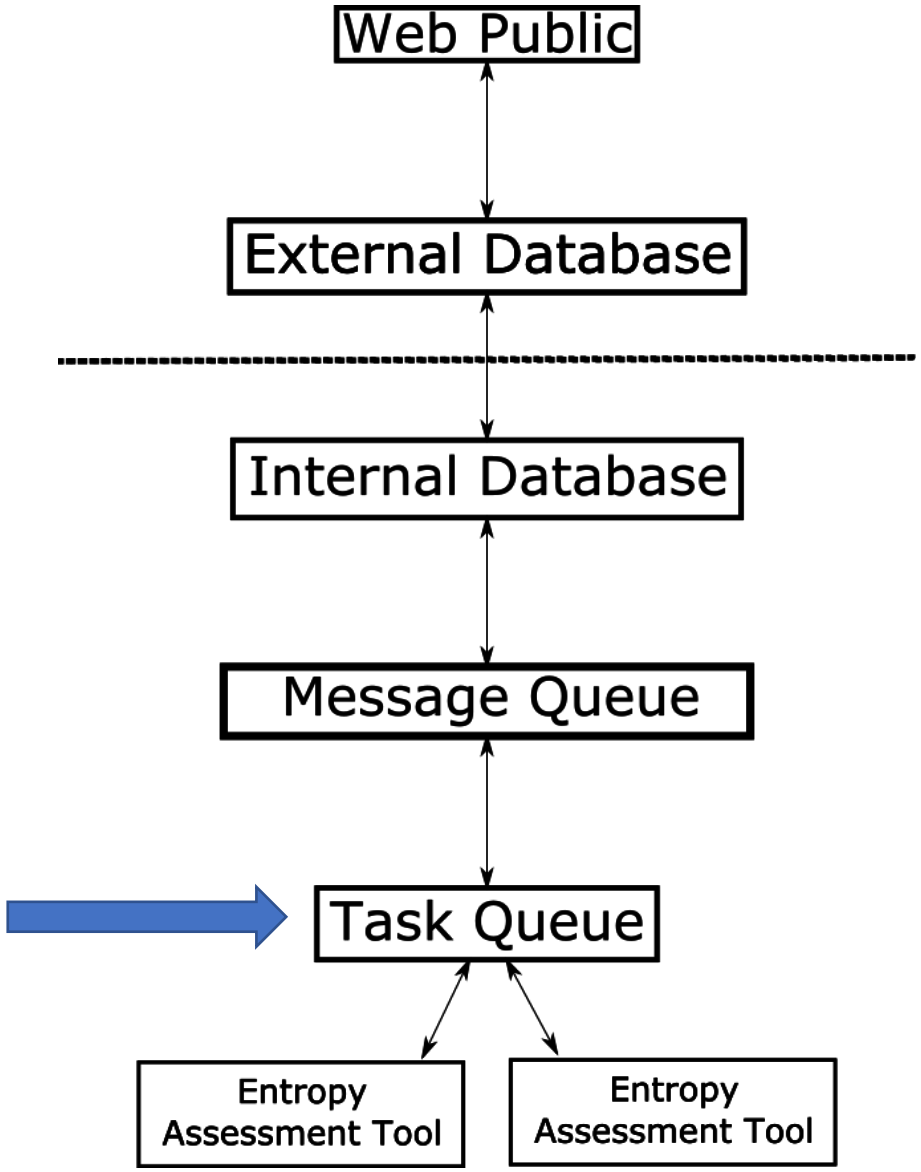
# Server Architecture – Message Queue




- Manages requests that CREATE or DELETE objects
- Objects need to percolate back to the public side
- Creates tasks for the Task Queue

- All messages process quickly but generated tasks might not

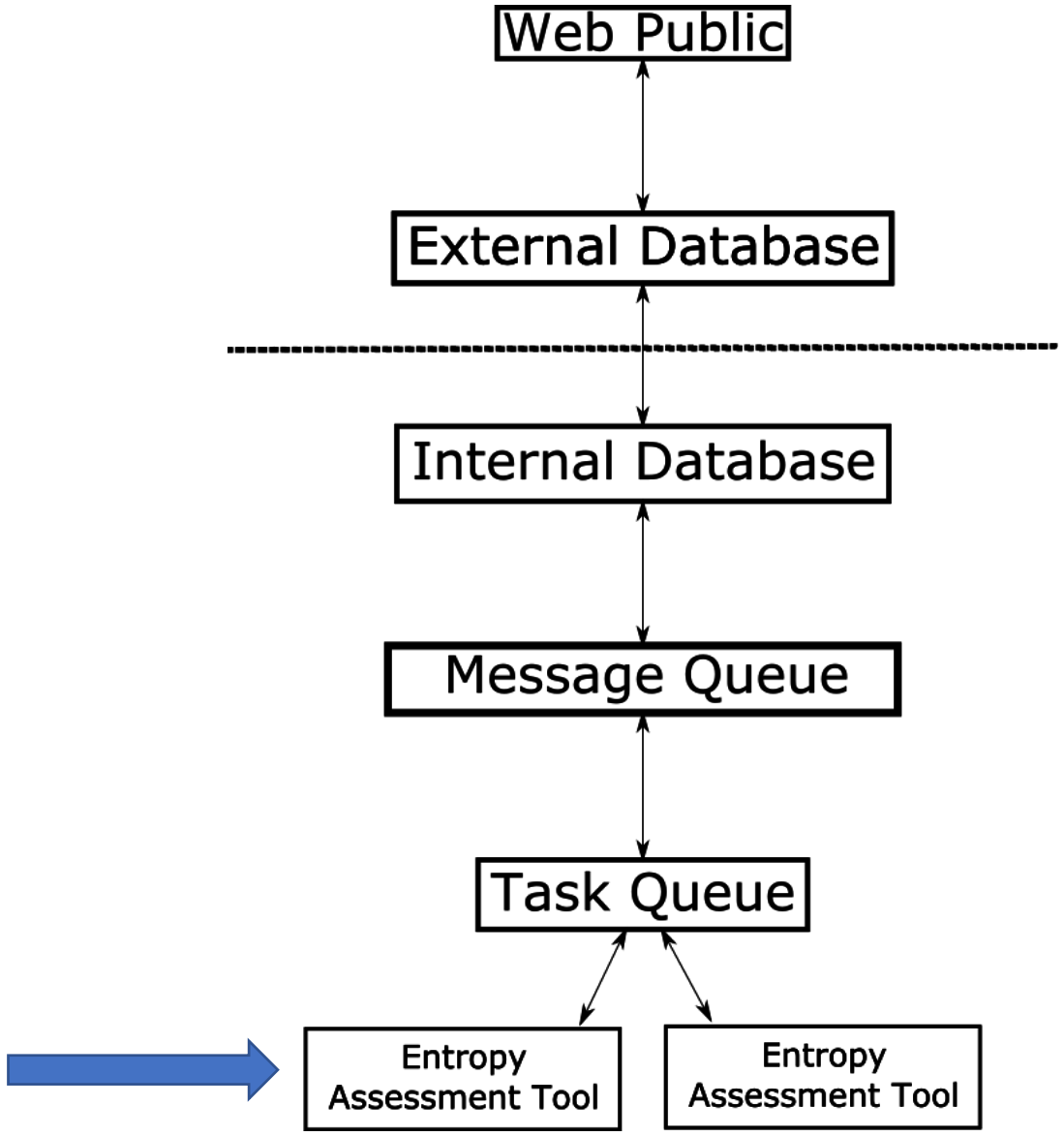
# Server Architecture – Task Queue




- Manages runs of the Entropy Assessment Tool
- Spins up Docker containers with the C++ code
- Stores results in database

- A run on a 10MB file (minimum size) takes a couple of minutes

# Server Architecture – Entropy Assessment Tool




- C++ implementation of tests as described in SP800-90B
- Available on GitHub: https://github.com/usnistgov/SP800-90B_EntropyAssessment

- Thanks to the contributors! Notably Joshua Hill, Kerry McKay, and Tim Hall

# Entropy Assessment Tool

- C++ (gcc) implementation of SP800-90B tests
- IID, non-IID, restart, conditioning testing available
- SP800-90B Sections 5 and 6
- IID testing tries to break the IID assumption by randomly permuting the data and running some statistical tests
  - Runs, median, periodicity, compression
  - Provides a min-entropy estimate from the most common value
- Non-IID testing conservatively estimates min-entropy
  - Lowest min-entropy estimate of all estimators is taken as the min-entropy

# ESV Demo – Authentication

```
[
  {
    "esvVersion": "1.0"
  },
  {
    "password": "12345678"
  }
]
```

Request Body

```
[
  {
    "esvVersion": "1.0"
  },
  {
    "accessToken":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJFPWNocmlzdG9waGVyLmNlbGlAbmlzdC5nb3YsIENOPUNocmlzIENlbGksIE9VPUVTViwgTz1OSVNULCBMPUdhaXRoZXJzYnVyZywgUz1NYXJ5bGFuZCwgQz1VUyIsIm5iZiI6MTYxOTUzNTUxMywiZXhwIjoxNjE5NTM3MzEzLCJpYXQiOjE2MTk1MzU1MTMsImlzcyI6Ik5JU1QgRVNWIERFTU8ifQ.S92_BXXzEBu_OqYCMSiCDE6MoXLKHiifsL6sfuKlg2E"
  }
]
```

Response Body

POST https://demo.esvts.nist.gov:7443/esv/v1/login

# ESV Demo – JWT

**Encoded** PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiJFPWNocmlzdG9waGVyLmNlbGlAbmlzd
C5nb3YsIENOPUNocmlzIENlbGksIE9VPUVTViwg
Tz1OSVNULCBMPUdhaXRoZXJzYnVyZywgUz1NYXJ
5bGFuZCwgQz1VUyIsIm5iZiI6MTYxOTUzNTUxMy
wiZXhwIjoxNjE5NTM3MzEzLCJpYXQiOjE2MTk1M
zU1MTMsImlzcyI6Ik5JU1QgRVNWIERFTU8ifQ.S
92_BXXzEBu_OqYCMSiCDE6MoXLKHiifsL6sfuKl
g2E
```

**Decoded** EDIT THE PAYLOAD AND SECRET

**HEADER:** ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

**PAYLOAD:** DATA

```
{
  "sub": "E=christopher.celi@nist.gov, CN=Chris Celi,
OU=ESV, O=NIST, L=Gaithersburg, S=Maryland, C=US",
  "nbf": 1619535513,
  "exp": 1619537313,
  "iat": 1619535513,
  "iss": "NIST ESV DEMO"
}
```

JSON Web Token unwrapped by https://jwt.io.

# ESV Demo – Registration


```
[
  {
    "esvVersion": "1.0”
  },
  {
    "primaryNoiseSource": "ring oscillators",
    "iidClaim": false,
    "bitsPerSample": 4,
    "alphabetSize": 16,
    "hminEstimate": 3.1,
    "physical": true,
    "itar": false,
    "rawNoiseSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "numberOfRestarts": 1000,
    "samplesPerRestart": 1000,
    "restartBitsSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "additionalNoiseSources": false,
    "conditioningComponent": [
      {
        "sequencePosition": 1,
        "vetted": false,
        "bijectiveClaim": false,
        "description": "parallel XOR-ed LFSRs with output buffer",
        "minNin": 16,
        "minHin": 4,
        "nw": 16,
        "nOut": 8,
        "conditionedBitsSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855”
      },
      {
        "sequencePosition": 2,
        "vetted": true,
        "description": "AES-CBC-MAC",
        "validationNumber": "A9876",
        "minNin": 128,
        "minHin": 4,
        "nw": 128,
        "nOut": 128
      }
    ]
  }
]
```


Request Body

POST https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments

# ESV Demo – Registration


```
[
  {
    "esvVersion": "1.0”
  },
  {
    "primaryNoiseSource": "ring oscillators",
    "iidClaim": false,
    "bitsPerSample": 4,
    "alphabetSize": 16,
    "hminEstimate": 3.1,
    "physical": true,
    "itar": false,
    "rawNoiseSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "numberOfRestarts": 1000,
    "samplesPerRestart": 1000,
    "restartBitsSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "additionalNoiseSources": false,
    "conditioningComponent": [
      {
        "sequencePosition": 1,
        "vetted": false,
        "bijectiveClaim": false,
        "description": "parallel XOR-ed LFSRs with output buffer",
        "minNin": 16,
        "minHin": 4,
        "nw": 16,
        "nOut": 8,
        "conditionedBitsSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855”
      },
      {
        "sequencePosition": 2,
        "vetted": true,
        "description": "AES-CBC-MAC",
        "validationNumber": "A9876",
        "minNin": 128,
        "minHin": 4,
        "nw": 128,
        "nOut": 128
      }
    ]
  }
]
```


Request Body

POST https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments

# ESV Demo – Registration


```
[
  {
    "esvVersion": "1.0”
  },
  {
    "primaryNoiseSource": "ring oscillators",
    "iidClaim": false,
    "bitsPerSample": 4,
    "alphabetSize": 16,
    "hminEstimate": 3.1,
    "physical": true,
    "itar": false,
    "rawNoiseSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "numberOfRestarts": 1000,
    "samplesPerRestart": 1000,
    "restartBitsSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "additionalNoiseSources": false,
    "conditioningComponent": [
      {
        "sequencePosition": 1,
        "vetted": false,
        "bijectiveClaim": false,
        "description": "parallel XOR-ed LFSRs with output buffer",
        "minNin": 16,
        "minHin": 4,
        "nw": 16,
        "nOut": 8,
        "conditionedBitsSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855”
      },
      {
        "sequencePosition": 2,
        "vetted": true,
        "description": "AES-CBC-MAC",
        "validationNumber": "A9876",
        "minNin": 128,
        "minHin": 4,
        "nw": 128,
        "nOut": 128
      }
    ]
  }
]
```


Request Body

POST https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments

# ESV Demo – Registration


```
[
  {
    "esvVersion": "1.0”
  },
  {
    "primaryNoiseSource": "ring oscillators",
    "iidClaim": false,
    "bitsPerSample": 4,
    "alphabetSize": 16,
    "hminEstimate": 3.1,
    "physical": true,
    "itar": false,
    "rawNoiseSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "numberOfRestarts": 1000,
    "samplesPerRestart": 1000,
    "restartBitsSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "additionalNoiseSources": false,
    "conditioningComponent": [
      {
        "sequencePosition": 1,
        "vetted": false,
        "bijectiveClaim": false,
        "description": "parallel XOR-ed LFSRs with output buffer",
        "minNin": 16,
        "minHin": 4,
        "nw": 16,
        "nOut": 8,
        "conditionedBitsSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855”
      },
      {
        "sequencePosition": 2,
        "vetted": true,
        "description": "AES-CBC-MAC",
        "validationNumber": "A9876",
        "minNin": 128,
        "minHin": 4,
        "nw": 128,
        "nOut": 128
      }
    ]
  }
]
```


Request Body

POST https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments

# ESV Demo – Registration


```
[
  {
    "esvVersion": "1.0”
  },
  {
    "primaryNoiseSource": "ring oscillators",
    "iidClaim": false,
    "bitsPerSample": 4,
    "alphabetSize": 16,
    "hminEstimate": 3.1,
    "physical": true,
    "itar": false,
    "rawNoiseSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "numberOfRestarts": 1000,
    "samplesPerRestart": 1000,
    "restartBitsSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "additionalNoiseSources": false,
    "conditioningComponent": [
      {
        "sequencePosition": 1,
        "vetted": false,
        "bijectiveClaim": false,
        "description": "parallel XOR-ed LFSRs with output buffer",
        "minNin": 16,
        "minHin": 4,
        "nw": 16,
        "nOut": 8,
        "conditionedBitsSHA256": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855”
      },
      {
        "sequencePosition": 2,
        "vetted": true,
        "description": "AES-CBC-MAC",
        "validationNumber": "A9876",
        "minNin": 128,
        "minHin": 4,
        "nw": 128,
        "nOut": 128
      }
    ]
  }
]
```


Request Body

POST https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments

# ESV Demo – Registration


```
[
  {
    "esvVersion": "1.0”
  },
  {
    "url": "/esvp/v1/entropyAssessments/20134",
    "createdOn": "2021-04-27T11:14:25.1890032-04:00",
    "expiresOn": "2021-04-27T11:14:25.1890051-04:00",
    "dataFileUrls": [
      {
        "rawNoiseBits": "/esvp/v1/entropyAssessments/20134/dataFiles/20324”
      },
      {
        "restartTestBits": "/esvp/v1/entropyAssessments/20134/dataFiles/20325”
      },
      {
        "conditionedBits": "/esvp/v1/entropyAssessments/20134/dataFiles/20326",
        "sequencePosition": 1
      }
    ],
    "publishable": false,
    "passed": false,
    "accessToken":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlYUlkIjoiMjAxMzQiLCJkZklkIjoiWzIwMzI0LDIwMzI1LDIwMzI2XSIsInN1Yi
I6IkU9Y2hyaXN0b3BoZXIuY2VsaUBuaXN0Lmdvdiwgq049Q2hyaXMgQ2VsaSwgT1U9RVNWLCBPPU5JU1QsIEw9R2FpdGhlcnNidXJnLC
BTPU1hcnlsYW5kLCBDPVVTIiwibmJmIjoxNjE5NTM2NDY1LCJleHAiOjE2MTk1MzgyNjUsImlhdCI6MTYxOTUzNjQ2NSwiaXNzIjoiTk
lTVCBFU1YgREVNTyJ9.9JZCdvZNzenALFz6BXg9RX8laGG-gGdVSHrY3Veprv4”
  }
]
```


Response Body

POST https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments

# ESV Demo – Registration


```
[
  {
    "esvVersion": "1.0”
  },
  {
    "url": "/esvp/v1/entropyAssessments/20134",
    "createdOn": "2021-04-27T11:14:25.1890032-04:00",
    "expiresOn": "2021-04-27T11:14:25.1890051-04:00",
    "dataFileUrls": [
      {
        "rawNoiseBits": "/esvp/v1/entropyAssessments/20134/dataFiles/20324”
      },
      {
        "restartTestBits": "/esvp/v1/entropyAssessments/20134/dataFiles/20325”
      },
      {
        "conditionedBits": "/esvp/v1/entropyAssessments/20134/dataFiles/20326",
        "sequencePosition": 1
      }
    ],
    "publishable": false,
    "passed": false,
    "accessToken":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlYUlkIjoiMjAxMzQiLCJkZklkIjoiWzIwMzI0LDIwMzI1LDIwMzI2XSIsInN1Yi
I6IkU9Y2hyaXN0b3BoZXIuY2VsaUBuaXN0Lmdvdiwgq049Q2hyaXMgQ2VsaSwgT1U9RVNWLCBPPU5JU1QsIEw9R2FpdGhlcnNidXJnLC
BTPU1hcnlsYW5kLCBDPVVTIiwibmJmIjoxNjE5NTM2NDY1LCJleHAiOjE2MTk1MzgyNjUsImlhdCI6MTYxOTUzNjQ2NSwiaXNzIjoiTk
lTVCBFU1YgREVNTyJ9.9JZCdvZNzenALFz6BXg9RX8laGG-gGdVSHrY3Veprv4”
  }
]
```


Response Body

POST https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments

# ESV Demo – Registration


```
[
  {
    "esvVersion": "1.0”
  },
  {
    "url": "/esvp/v1/entropyAssessments/20134",
    "createdOn": "2021-04-27T11:14:25.1890032-04:00",
    "expiresOn": "2021-04-27T11:14:25.1890051-04:00",
    "dataFileUrls": [
      {
        "rawNoiseBits": "/esvp/v1/entropyAssessments/20134/dataFiles/20324”
      },
      {
        "restartTestBits": "/esvp/v1/entropyAssessments/20134/dataFiles/20325”
      },
      {
        "conditionedBits": "/esvp/v1/entropyAssessments/20134/dataFiles/20326",
        "sequencePosition": 1
      }
    ],
    "publishable": false,
    "passed": false,
    "accessToken":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlYUlkIjoiMjAxMzQiLCJkZklkIjoiWzIwMzI0LDIwMzI1LDIwMzI2XSIsInN1Yi
I6IkU9Y2hyaXN0b3BoZXIuY2VsaUBuaXN0LmdvdiwgQ049Q2hyaXMgQ2VsaSwgT1U9RVNWLCBPPU5JU1QsIEw9R2FpdGhlcnNidXJnLC
BTPU1hcnlsYW5kLCBDPVVTIiwibmJmIjoxNjE5NTM2NDY1LCJleHAiOjE2MTk1MzgyNjUsImlhdCI6MTYxOTUzNjQ2NSwiaXNzIjoiTk
lTVCBFU1YgREVNTyJ9.9JZCdvZNzenALFz6BXg9RX8laGG-gGdVSHrY3Veprv4”
  }
]
```


Response Body

POST https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments

# ESV Demo – JWT

**Encoded** PASTE A TOKEN HERE


```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JlYUlkIjoiMjAxMzQiLCJkZklkIjoiWzIwMzI0L
DIwMzI1LDIwMzI2XSIsInN1YiI6IkU9Y2hyaXN0
b3BoZXIuY2VsaUBuaXN0LmdvdiwgQ049Q2hyaXM
gQ2VsaSwgT1U9RVNWLCBPPU5JU1QsIEw9R2FpdG
hlcnNidXJnLCBTPU1hcnlsYW5kLCBDPVVTIiwib
mJmIjoxNjE5NTM2NDY1LCJleHAiOjE2MTk1Mzgy
NjUsImlhdCI6MTYxOTUzNjQ2NSwiaXNzIjoiTkl
TVCBFU1YgREVNTyJ9.9JZCdvZNzenALFz6BXg9R
X8laGG-gGdVSHrY3Veprv4
```


**Decoded** EDIT THE PAYLOAD AND SECRET

**HEADER:** ALGORITHM & TOKEN TYPE

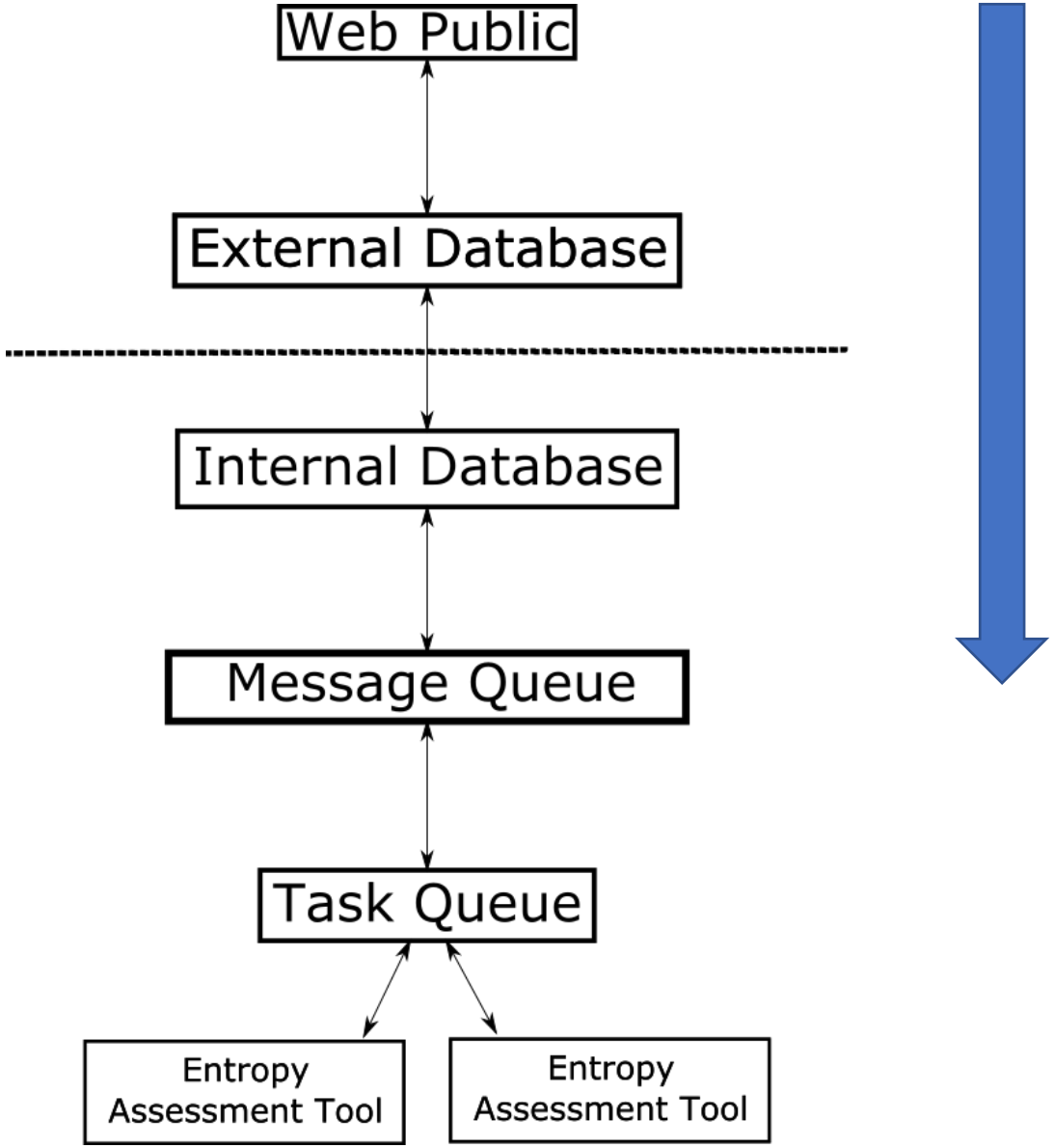

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```


**PAYLOAD:** DATA


```
{
  "eaId": "20134",
  "dfId": "[20324,20325,20326]",
  "sub": "E=christopher.celi@nist.gov, CN=Chris Celi,
OU=ESV, O=NIST, L=Gaithersburg, S=Maryland, C=US",
  "nbf": 1619536465,
  "exp": 1619538265,
  "iat": 1619536465,
  "iss": "NIST ESV DEMO"
}
```


JSON Web Token unwrapped by https://jwt.io.

# ESV Demo – Registration



# ESV Demo – DataFile Upload

```
POST /esv/v1/entropyAssessments/20134/dataFiles/20324 HTTP/1.1

Host: demo.esvts.nist.gov:7443

Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlYUlkIjoiMjAxMzQiLCJkZklkIjoiWzIwMzI0LDIwMzI1LDIwMzI2XSIsInN1YiI
6IkU9Y2hyaXN0b3BoZXIuY2VsaUBuaXN0Lmdvdiwg049Q2hyaXMgQ2VsaSwgT1U9RVNWLCBPPU5JU1QsIEw9R2FpdGhlcnNidXJnLCB
TPU1hcnlsYW5kLCBDPVVTIiwibmJmIjoxNjE5NTM2NDY1LCJleHAiOjE2MTk1MzgyNjUsImlhdCI6MTYxOTUzNjQ2NSwiaXNzIjoiTkl
TVCBFU1YgREVNTyJ9.9JZCdvZNzenALFz6BXg9RX8laGG-gGdVSHrY3Veprv4

Content-Length: 201

Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW


----WebKitFormBoundary7MA4YWxkTrZu0gW

Content-Disposition: form-data; name="dataFile"; filename="truerand_4bit.bin"

Content-Type: application/octet-stream

(data)

----WebKitFormBoundary7MA4YWxkTrZu0gW
```

Request Body

POST https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments/<eaId>/dataFiles/<dfId>

# ESV Demo – DataFile Upload

```
[
  {
    "esvVersion": "1.0”
  },
  {
    "uploadType": "UploadDataFile",
    "status": "success",
    "dataLengthBytes": 1000000
  }
]
```

Response Body

POST https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments/<eaId>/dataFiles/<dfId>

# ESV Demo – DataFile Status

```
[
    {
        "esvVersion": "1.0”
    },
    {
        "dataFileID": 20324,
        "status": "initial",
    }
]
```

Response Body

GET https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments/<eaId>/dataFiles/<dfId>

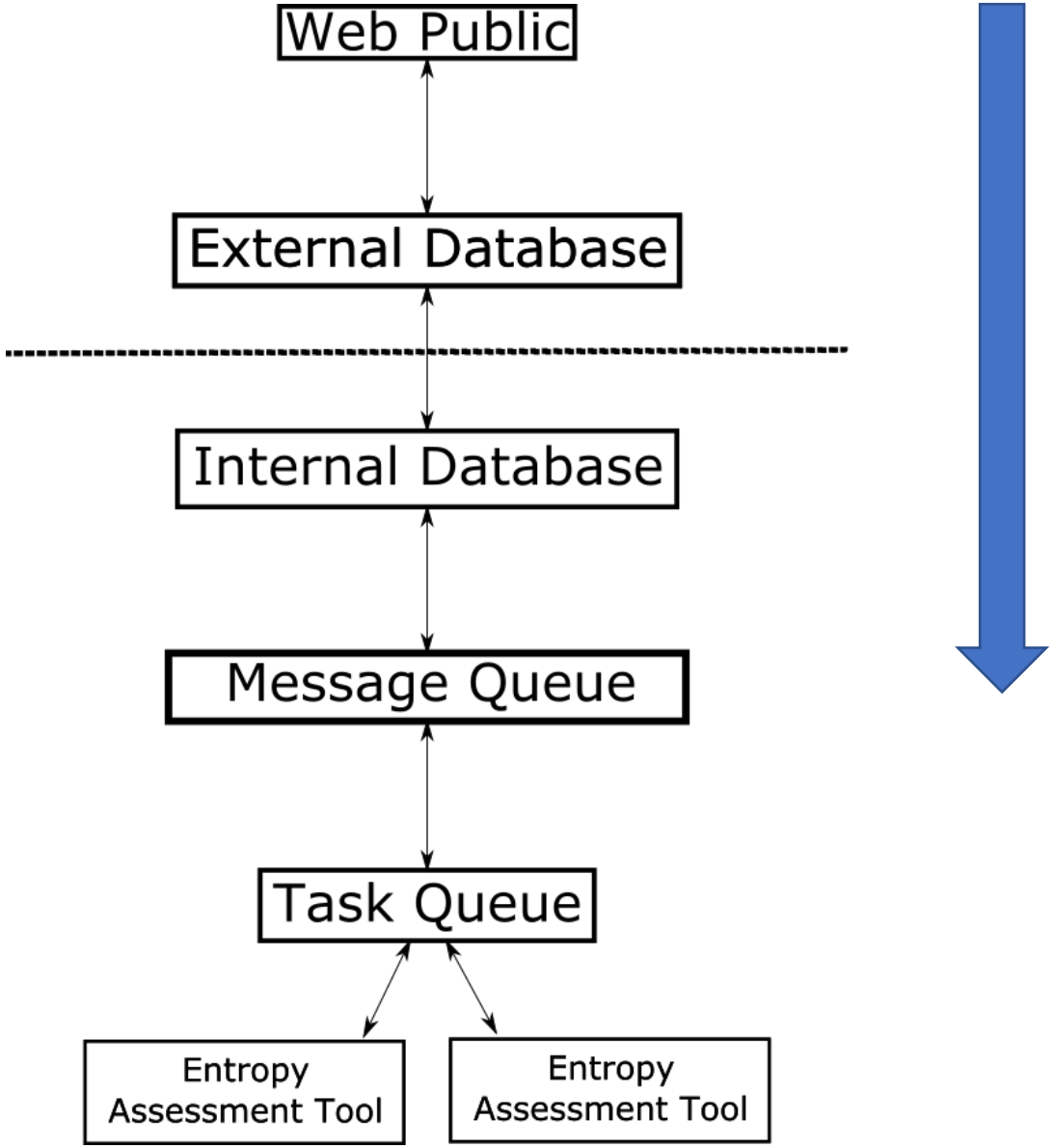
# ESV Demo – DataFile Status

```
[
    {
        "esvVersion": "1.0”
    },
    {
        "dataFileID": 20324,
        "status": ”uploaded",
    }
]
```

Response Body

GET https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments/<eaId>/dataFiles/<dfId>

# ESV Demo – DataFile Upload



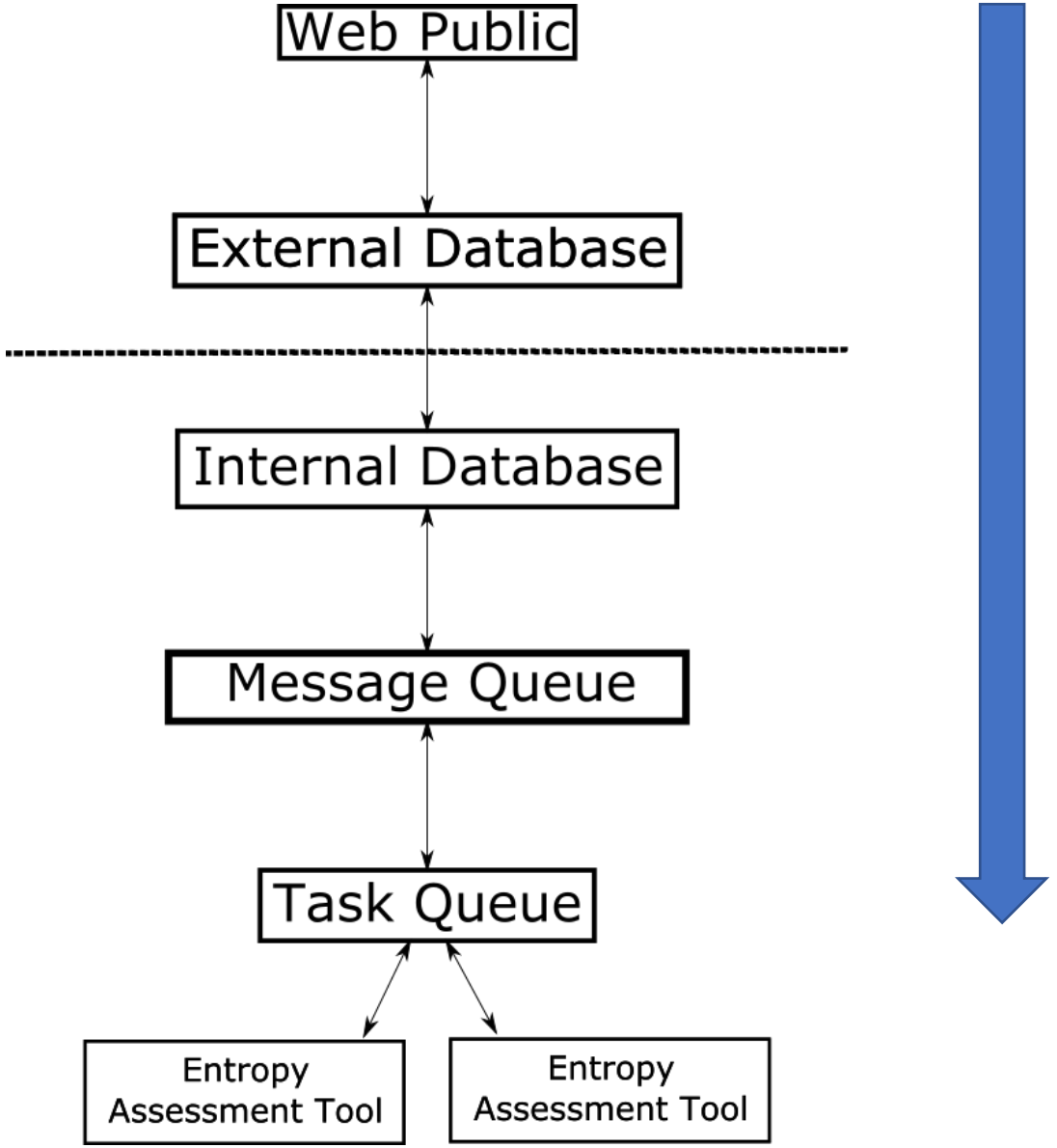
# ESV Demo – DataFile Status


```
[
    {
        "esvVersion": "1.0”
    },
    {
        "dataFileID": 20324,
        "status": "started",
        "sha256":
"489bc841bb364ba86da70b1617138aef76b25dd9196ad669eef40c1441b6cb88"
    }
]
```


Response Body

GET https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments/<eaId>/dataFiles/<dfId>

# ESV Demo – DataFile Upload



# ESV Demo – DataFile Status


```
[
    {
        "esvVersion": "1.0”
    },
    {
        "dataFileID": 20324,
        "status": "success",
        "sha256": "489bc841bb364ba86da70b1617138aef76b25dd9196ad669eef40c1441b6cb88",
        "testCases": [
            {
                "testCaseDesc": "Estimate entropy with Most Common Value",
                "hOriginal": 3.9711943367296096,
                "hBitstring": 0.9977303858221566,
                "hAssessed": -1,
                "retMinEntropy": 3.9711943367296096,
                "dataWordSize": 4

...
```


Response Body

GET https://demo.esvts.nist.gov:7443/esv/v1/entropyAssessments/<eaId>/dataFiles/<dfId>

# ESV Demo – Supporting Documentation

```
POST /esv/v1/supportingDocumentation HTTP/1.1
Host: demo.esvts.nist.gov:7443
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlYUlkIjoiMjYiLCJkZklkIjoiWzc2LDc3LDc4XSIsInN1YiI6IkU9ZXN2LmNsaWV
udEBuaXN0Lmdvdiwgg049RVNWIENsaWVudCBEZXZlbG9wZXIsIE9VPUVTViBMb2NhbCBDbGllbnQsIE89TklTVCwgTD1HYWl0aGVyc2J
1cmcsIFM9TWFyeWxhbmQsIEM9VVMiLCJuYmYiOjE2MTk1NjQ3MTUsImV4cCI6MTYxOTU2NjUxNSwiaWF0IjoxNjE5NTY0NzE1LCJpc3M
iOiJOSVNUIEVTViBMT0NBTCJ9.r_i3YLVhDZyAkmtQMiHjOW0EgFQJdJa59pJ2s836B38

Content-Length: 374
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW



----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="itar”
off
----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="sdComments”
My comments.
----WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="sdFile"; filename="Test PDF.pdf”
Content-Type: application/pdf
(data)
----WebKitFormBoundary7MA4YWxkTrZu0gW
```

Request Body

POST https://demo.esvts.nist.gov:7443/esv/v1/supportingDocumentation

# ESV Demo – Supporting Documentation


```
[
  {
    "esvVersion": "1.0”
  },
  {
    "sdId": 20002,
    "uploadType": "UploadSupportingDocumentation",
    "status": "success",
    "dataLengthBytes": 30133,
    "accessToken":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzZElkIjoiMjAwMDIiLCJzdWIiOiJFPWVzdi5j
bGllbnRAbmlzdC5nb3YsIENOPUVTViBDbGllbnQgRGV2ZWxvcGVyLCBPVT1FU1YgTG9jYWwgQ2xpZW
50LCBPPU5JU1QsIEw9R2FpdGhlcnNidXJnLCBTPU1hcnlsYW5kLCBDPVVTIiwibmJmIjoxNjE5NTY0
NzI4LCJleHAiOjE2MTk1NjY1MjgsImlhdCI6MTYxOTU2NDcyOCwiaXNzIjoiTklTVCBFU1YgTE9DQU
wifQ.v6Twy1k34lxya2OMzV343BgQ3R9nXAsa55lT3oufXyg”
  }
]
```


Response Body

POST https://demo.esvts.nist.gov:7443/esv/v1/supportingDocumentation

# ESV Demo – JWT

**Encoded** PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzZElkIjoiMjAwMDIiLCJzdWIiOiJFPWVzdi5jb
GllbnRAbmlzdC5nb3YsIENOPUVTViBDbGllbnQg
RGV2ZWxvcGVyLCBPVT1FU1YgTG9jYWwgQ2xpZW5
0LCBPPU5JU1QsIEw9R2FpdGhlcnNidXJnLCBTPU
1hcnlsYW5kLCBDPVVTIiwibmJmIjoxNjE5NTY0N
zI4LCJleHAiOjE2MTk1NjY1MjgsImlhdCI6MTYx
OTU2NDcyOCwiaXNzIjoiTklTVCBFU1YgTE9DQUw
ifQ.v6Twy1k34lxya2OMzV343BgQ3R9nXAsa55l
T3oufXyg
```

**Decoded** EDIT THE PAYLOAD AND SECRET

**HEADER:** ALGORITHM & TOKEN TYPE

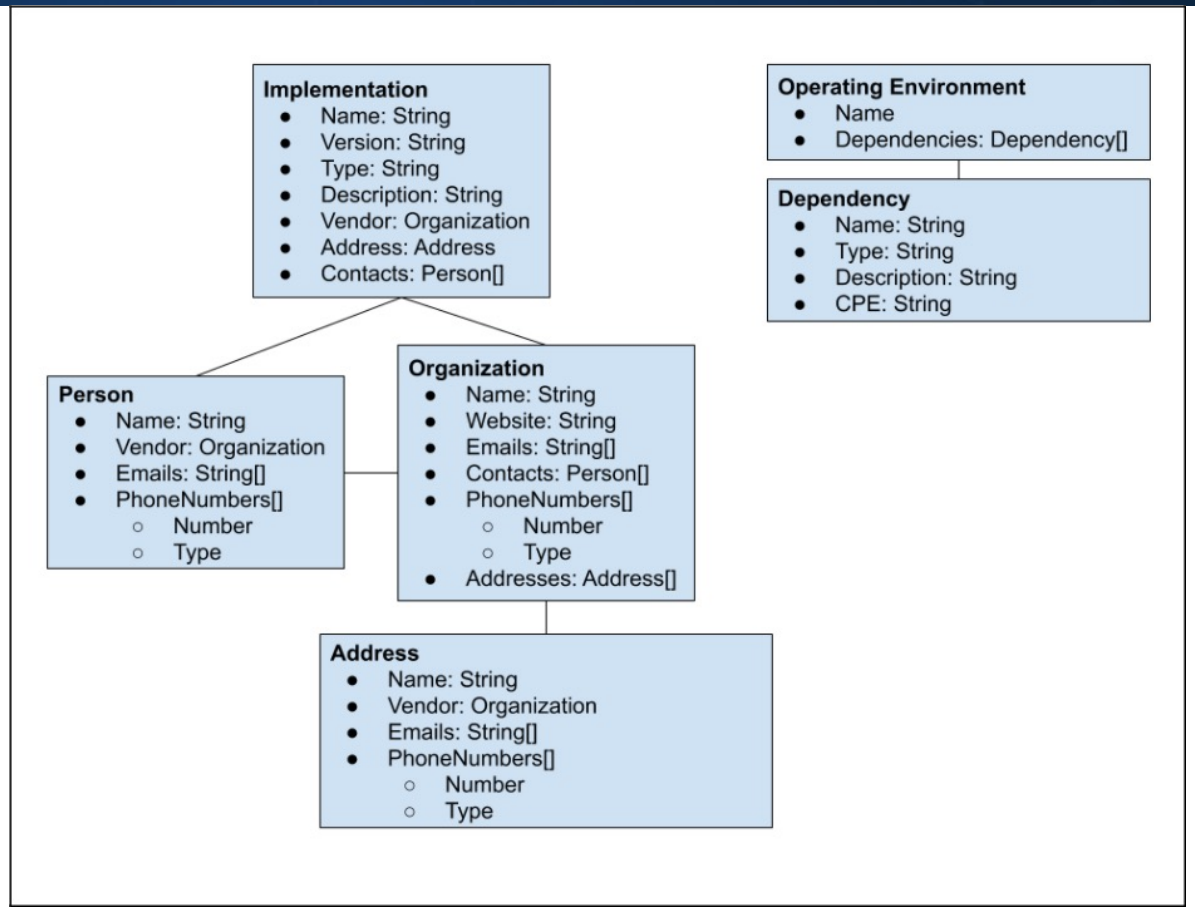
```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

**PAYLOAD:** DATA

```
{
  "sdId": "20002",
  "sub": "E=esv.client@nist.gov, CN=ESV Client
Developer, OU=ESV Local Client, O=NIST, L=Gaithersburg,
S=Maryland, C=US",
  "nbf": 1619564728,
```

JSON Web Token unwrapped by https://jwt.io.

# ESV Demo – Module Information




Using ACVTS to upload and approve general information about the platform and developer

# ESV Demo – Certify

```
[
  {
    "esvVersion": "1.0”
  },
  {
    "itar": false,
    "limitEntropyAssessmentToSingleModule": false,
    "moduleId": 1,
    "vendorId": 1,
    "supportingDocumentation": [
      {
        "sdId": 2460095,
        "accessToken": ”…”
      },
      {
        "sdId": 2460096,
        "accessToken": ”…”
      }
    ],
    "entropyAssessments": [
      {
        "eaId": 67,
        "oeId": 1,
        "accessToken": ”…”
      }
    ]
  }
]
```

Request Body

POST https://demo.esvts.nist.gov:7443/esv/v1/certify

# ESV Demo – Certify

```
[
  {
    "esvVersion": "1.0”
  },
  {
    "itar": false,
    "limitEntropyAssessmentToSingleModule": false,
    "moduleId": 1,
    "vendorId": 1,
    "supportingDocumentation": [
      {
        "sdId": 2460095,
        "accessToken": ”…”
      },
      {
        "sdId": 2460096,
        "accessToken": ”…”
      }
    ],
    "entropyAssessments": [
      {
        "eaId": 67,
        "oeId": 1,
        "accessToken": ”…”
      }
    ]
  }
]
```

Request Body

POST https://demo.esvts.nist.gov:7443/esv/v1/certify

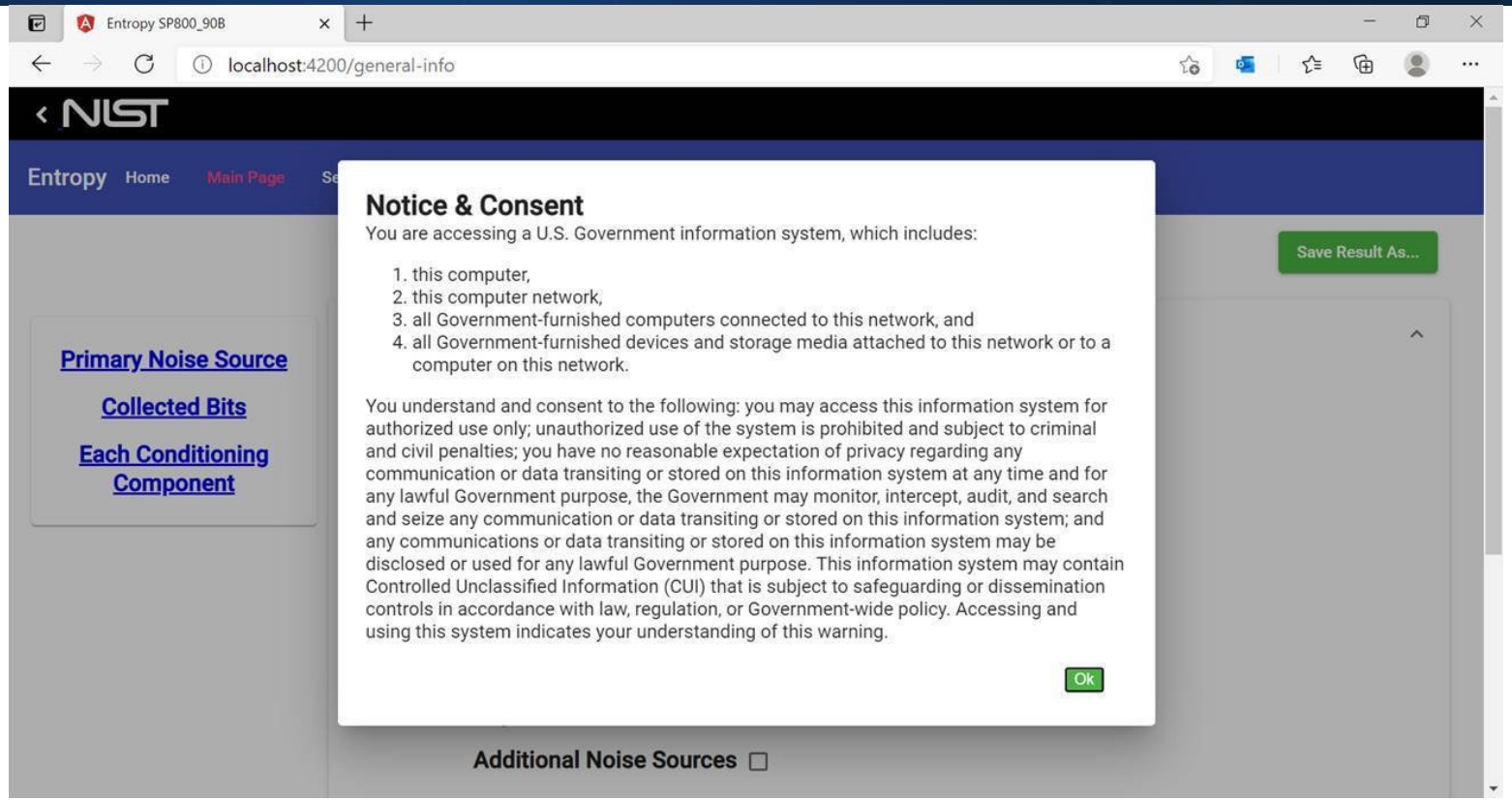
# ESV Demo – Certify


```
[
  {
    "esvVersion": "1.0”
  },
  {
    "status": "received",
    "information": {
      "messageList": [
        "vendorId name is EXAMPLE VENDOR.",
        "moduleId name is EXAMPLE MODULE NAME.”
      ],
      "entropyAssessmentsReferences": {
        "elementList": [
          {
            "location": "indexPosition:1",
            "messageList": [
              "oeId name is EXAMPLE OE."
            ]
          }
        ]
      }
    }
  }
]
```


Response Body

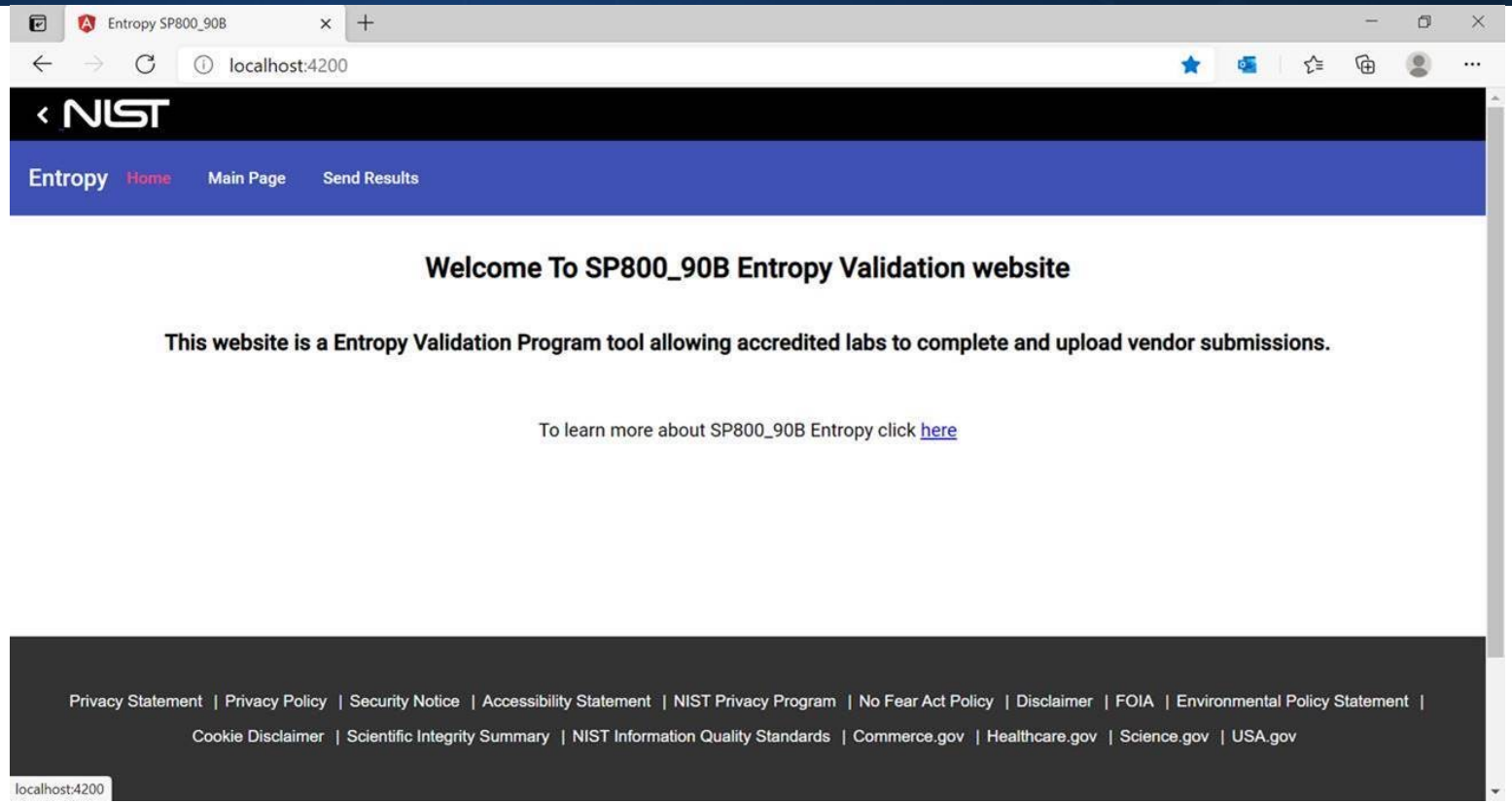
POST https://demo.esvts.nist.gov:7443/esv/v1/certify

# ESV HTTP Client



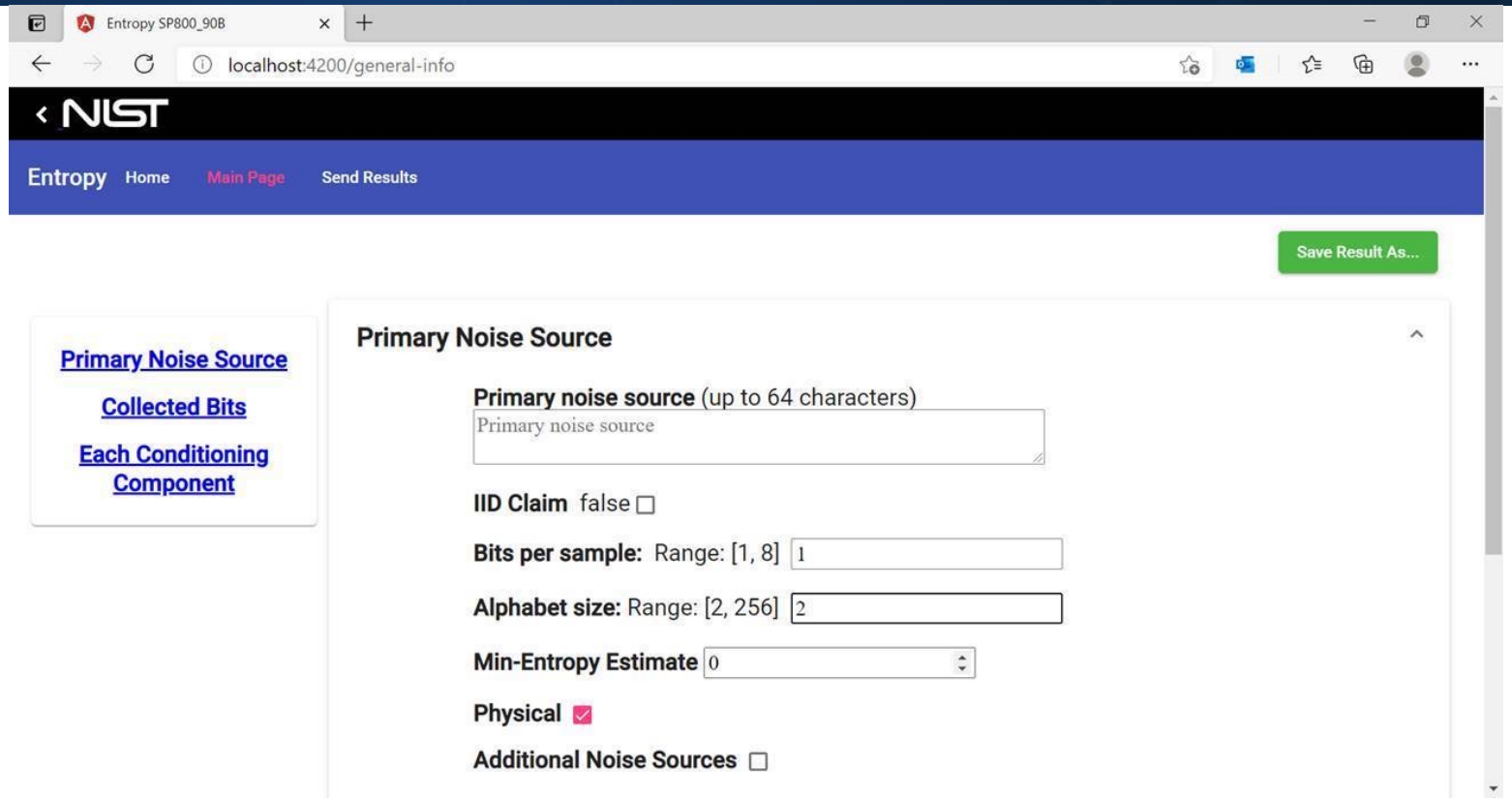

Client is a work in progress, screenshots may not represent final result.

# ESV HTTP Client



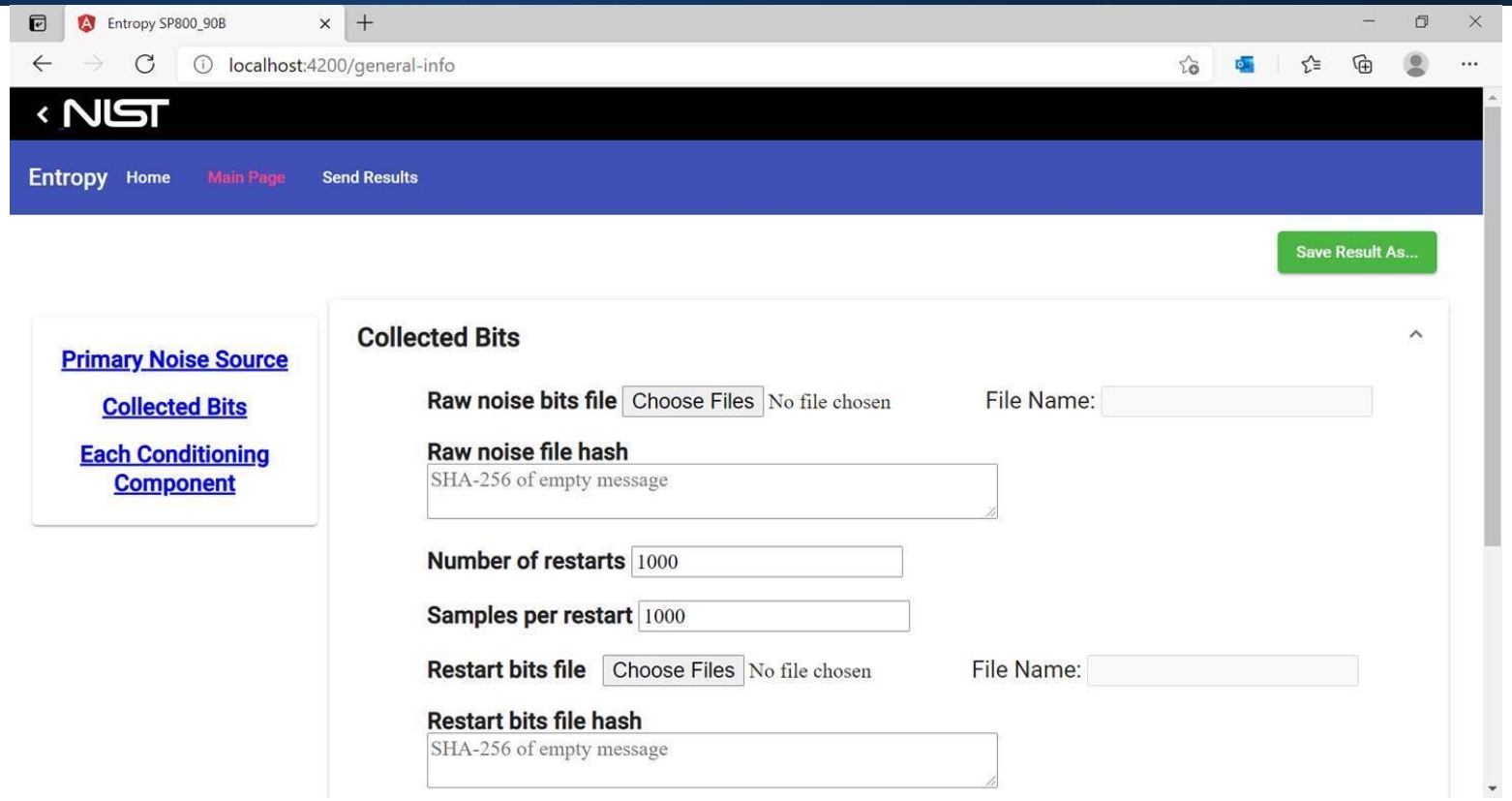

Client is a work in progress, screenshots may not represent final result.

# ESV HTTP Client



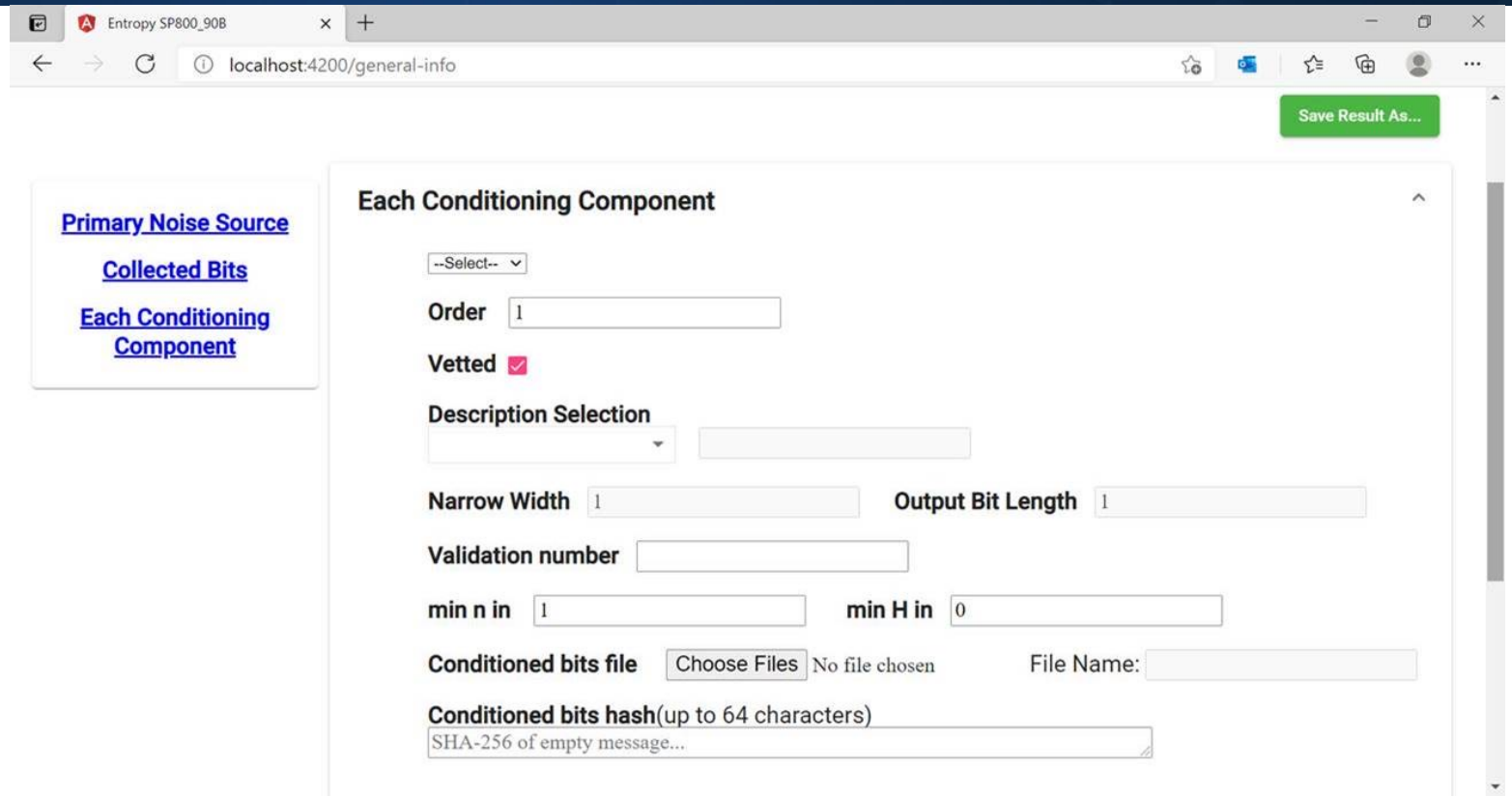

Client is a work in progress, screenshots may not represent final result.

# ESV HTTP Client




Client is a work in progress, screenshots may not represent final result.

# ESV HTTP Client




Client is a work in progress, screenshots may not represent final result.

# Questions?

https://github.com/usnistgov/ESV-Server
https://github.com/usnistgov/SP800-90B_EntropyAssessment