INTERFACE SPECIFICATION

FOR

CONSENT BASED SSN VERIFICATION

(CBSV) WEB SERVICE

RELEASE NUMBER: 1.0

AUGUST 27, 2010
LIST OF FIGURES

Figure 1: CBSV Web Service Ping Process Data Flow................................................................. 10
Figure 2: CBSV Web Service Verify Process Data Flow.............................................................. 11
Figure 3: CBSV Web Service Verify Process Data Flow............................................................. 12
1.0 INTRODUCTION

The Consent Based Social Security Number (SSN) Verification (CBSV) Web Service application allows the name and SSN of individuals to be verified against the Social Security Administration’s (SSA’s) master data file.

A CBSV Web Service user, referred to as the “Requesting Party” throughout this document, must develop a Web Service client to interface with SSA’s CBSV Web Service application. SSA offers limited technical customer support and recommends that the Requesting Party have the expertise to build and support the CBSV Web Service client software.

This document identifies the interface specifications between a Requesting Party and the CBSV Web Service and describes in detail the exchange of data in the form of requests and responses in order to allow Requesting Parties to develop their Web Service client software. An overview of SSA’s architectural components that interact with the CBSV Web Service is also provided.
2.0 CBSV WEB SERVICE FUNCTION OVERVIEW

The CBSV Web Service application verifies whether a submitted name and SSN combination matches SSA’s records for any business or other entity (i.e., user) that has registered to use the service and has obtained the written consent of the number holder.

Once the Requesting Party’s submission passes SSA’s finance and agreement checks, CBSV Web Service returns verification results with status codes including:

- “0000” to indicate that the information submitted matches SSA’s records,
- “9991” to indicate that the information submitted does not match SSA’s records, or
- “0001” to indicate that, according to SSA’s records, the number holder is deceased.

Specific information about which data elements did not match SSA records will not be available.

The CBSV Web Service provides real-time results for name/SSN combinations, one at a time. As part of the Web Service request process, the Web Service client must submit the Web Service User Identifier (ID) and password, as well as the data that is to be verified, which is encrypted within the SOAP message. The CBSV Web Service returns a failure response if the Web Service request SOAP message contains any data that the SSA interface restricts as keywords. In such instances, the Requesting Party can use the CBSV online service for name/SSN verification as an alternative. It is recommended that the requesting party register for a CBSV online user ID and password at the time of registration for the CBSV Web Service User ID and password. For the online registration process, please refer to the CBSV User Guide, available at [http://www.ssa.gov/cbsv/library.html](http://www.ssa.gov/cbsv/library.html).
3.0 SSA PROCEDURAL PREREQUISITES

In order to be eligible to use the CBSV Web Service interface, the following CBSV registration criteria must have been met, as per SSA guidelines:

- A $5,000 registration fee must be paid,
- Form SSA-88 (Pre-Approval form for CBSV) must be completed by the designated company official and approved by SSA,
- Form SSA-1235 (the user agreement between SSA and the Requesting Party for use of CBSV) must be completed by the designated company official and approved by SSA, and
- The registration process must be completed via SSA’s Integrated Registration Services (IRES) Business Service Online (BSO) application to obtain a CBSV Web Service user ID and password and to get the CBSV Web Service role activated. A manager or authorized representative must register for a Web Service user ID and password on behalf of the Requesting Party.

Note: The CBSV Web Service user ID and password cannot be used for the CBSV online or batch service. The Requesting Party will need to register, at no added cost, for additional user ID(s) to access the CBSV online and batch services.
4.0 GENERAL TECHNICAL PREREQUISITES

The following technical prerequisites must be satisfied by the Requesting Party to use the CBSV Web Service:

- Provision of a X.509 digital certificate public key that will be used to sign the request SOAP message. The certificate must be acquired from a recognized, trusted Certificate Authority (CA).
- Establishment of a Web Service development environment that supports using the .NET and/or Java-based programming language technologies.
5.0 WEB SERVICE INTERFACE REQUIREMENTS

Development of Web Service clients for Web Service transactions requires the following technical characteristics:

- Conformance to World Wide Web Consortium (W3C) Web Service standards, including SOAP, Web Services Description Language (WSDL), and Web Services Security (WS-Security, also known as WSS).

- CBSV Web Service secures communication and transactions conducted with the CBSV Web Service client applications, by enabling security over the transport layer using the Hypertext Transfer Protocol Secure (HTTPS) employing Secure Sockets Layer (SSL) certificates signed by well-known, trusted CAs. It is recommended that the CBSV Web Service client must be configured to trust:
  - CA root certificate; and/or
  - CA intermediate certificate(s). The CBSV Web Service Client should not be configured to trust a specific certificate.

- WSS implemented using the following authentication mechanisms:
  - Client authentication using the Web Service user ID and password as part of the WSS SOAP header, and
  - Strong authentication (using X.509 client certificates), which authenticates the Requesting Party based on a digital signature over the SOAP: body and a timestamp element.
6.0 INTERFACE OPERATIONS

CBSV Requesting Parties must register for a user ID and password with SSA via the IRES BSO application prior to using the CBSV Web Service. They must also acquire an X.509 certificate from a recognized, trusted CA and provide SSA with a public key for this certificate prior to using the Web Service. WSS is used in tandem with an X.509 certificate.

Requesting Parties must notify SSA of the authorized employee’s name whose Form SSA-88 will be used to request access to the CBSV Web Service. The Requesting Party can verify one name/SSN per request; every request must be a separate Web Service call.

Data is exchanged between the Requesting Party application and SSA using the CBSV Web Service. The CBSV Web Service WSDL required to secure the exchange of data is available at https://ws.ssa.gov/CBSVWS/services/CBSVServices?wsdl.

The CBSV Web Service provides two operations:

- **ping**: The ping operation is used to determine if the required SSA resources are available. Requesting Party’s credentials are used to authenticate the request. *(Refer to Figure 1 - CBSV Web Service Ping Process Data Flow.)*

- **verify**: The verify operation compares the data provided by the Requesting Party with the data in the SSA master files. *(Refer to Figures 2 and 3 - CBSV Web Service Verify Process Data Flow.)*
7.0 SEQUENCE OF REQUESTS AND RESPONSES

The following diagrams (Figure 1 for the ping operation and Figures 2 and 3 for the verify operation) show the typical sequence of requests and responses between the CBSV Requesting Parties and the CBSV Web Service architectural components.

Upon receiving a request, several preliminary validations are performed. Validations include the following:

- **Schema Validation** – Ensuring that the request data is in accordance with the format specified in the schema.
- **Authentication** – Confirming the identity (user ID and password) of the Requesting Party.
- **Authorization** – Once authenticated, ensuring the Requesting Party is authorized to perform the requested operation.

If any of the preliminary validations return a negative result, the requested operation cannot be performed.

If the preliminary validations are successful and return positive confirmations, the requested operation may be performed. Specific responses for each operation are described in Section 8.0.
Figure 1: CBSV Web Service Ping Process Data Flow
Figure 2: CBSV Web Service Verify Process Data Flow
(Continued in Figure 3)
# Interface Specification for Consent Based SSN Verification Web Service

## Figure 3: CBSV Web Service Verify Process Data Flow

<table>
<thead>
<tr>
<th>Requesting Party</th>
<th>SSA DataPower</th>
<th>SSA ACU/RES</th>
<th>SSA CBSV Websphere</th>
<th>SSA Finance &amp; Agreement (F&amp;A)</th>
<th>SSA Mainframe</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Verify

- **Requesting Party**
  - Receives Finance & Agreement Failure message
  - Receives Success or Failure Status Code

- **SSA DataPower**
  - Invoke F & A Verification Check
  - Performs F & A Check
  - Return F & A Check Status

- **SSA ACU/RES**
  - Evaluate F & A Response
  - Returns F & A Response to Requesting Party

- **SSA CBSV Websphere**
  - Invocation of Mainframe Program for SSN Verification
  - Send SSN Verification Result Response to Requesting Party

- **SSA Finance & Agreement (F&A)**
  - Perform SSN Verification
  - Return SSN Verification Result Code

---

Interface Specification for CBSV Web Service

12

08/27/2010
8.0 STRUCTURE OF REQUESTS AND RESPONSES

Requesting Parties must use the WSDL provided by SSA for Web Service client development. Information regarding the input and output parameters for the CBSV Web Service operations is contained in the WSDL, which is provided in Section 9.0.

SSA uses SOAP and WSS. SOAP headers that include credentials are required in all requests (see example of the SOAP header required for a specific request in Section 8.2.1.1).

The following WSS mechanisms are required to conduct secure SOAP message exchanges with the CBSV Web Service:

- The SOAP header must conform to the Web Services Security “UsernameToken Profile.” It must contain a UsernameToken of type wsse: Username with an appropriate password of type wsse: PasswordText.
- The SOAP message must be signed, conforming to “Web Services Security: SOAP Message Security” guidance.
- To sign the SOAP message digitally, the Requesting Party will need an X.509 certificate from a trusted CA (e.g., DigiCert, VeriSign, Entrust, etc.) or an internal CA. The Requesting Party must provide SSA with a public key for this certificate.

The Requesting Party must email the “.cer” file that contains the public key for their X.509 certificate to SSA at web.service.testing@ssa.gov. The .cer extension of the certificate must be changed to .txt before sending, or the file can be emailed using compression software with a “.zip” extension.

8.1 OVERVIEW OF REQUESTS

<table>
<thead>
<tr>
<th>Operation</th>
<th>Major data elements sent with the request</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping</td>
<td>The Requesting Party’s credentials in SOAP header</td>
<td>8.2.1</td>
</tr>
<tr>
<td>verify</td>
<td>The Requesting Party’s credentials in SOAP header as well as SSN, name, and other optional data as verify parameters in SOAP body</td>
<td>8.3.1</td>
</tr>
</tbody>
</table>

8.2 PING REQUEST AND RESPONSE STRUCTURE

The ping operation is used to determine if the SSA resources are available. The Requesting Party’s credentials are used to authenticate the request.
### 8.2.1 Request

The following data elements will be sent in the SOAP header of the ping operation request (refer to the examples for attributes that may be required to support these parent elements):

<table>
<thead>
<tr>
<th>Element</th>
<th>Value Required</th>
<th>Value Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;wsse: SecurityTokenReference&gt;</code></td>
<td>Required</td>
<td>Value is the public key of the certificate</td>
<td>See example in Section 8.2.1.1</td>
</tr>
<tr>
<td><code>&lt;wsse:UsernameToken&gt;</code></td>
<td>Required</td>
<td>Includes eight-digit <code>&lt;Username&gt;</code> and <code>&lt;Password&gt;</code>; see example for child elements that may be required (such as Nonce, Created)</td>
<td>See example in Section 8.2.1.1</td>
</tr>
<tr>
<td><code>&lt;ds:Signature xmlns=&quot;http://www.w3.org/2000/09/xmldsig#&quot;</code></td>
<td>Required</td>
<td>See example for child elements that may be required</td>
<td>See example in Section 8.2.1.1</td>
</tr>
</tbody>
</table>

The `<Username>` tag contains the Requesting Party’s User ID, which is alpha-numeric and eight characters in length.

The `<Password>` tag contains the Requesting Party’s password. It must be eight characters in length, must contain all uppercase letters, and must be alpha-numeric.

#### 8.2.1.1 PING Request SOAP Header

```xml
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
    <ds:Signature Id="Signature-16260234" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
```

<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#id-1934804">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>nfdqOvUMsiWz4OJva/einMCM/x0=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
JAJMc6Qt5K9KZssnEG8v3rts7oTr7dBjMte3XwkckMYW1wha69oFx6DqaXncjd3Uk3oKuD1B
aPDD
bustMxNYxpJ7zYM/KCCWYc4j2j4PQ6rXURQ7flyAL7qzBxqHL8Eh28FxYKtwcdw780HAM
R8sSSIb
WEZzd7/rIw54izU87xI=
</ds:SignatureValue>
<ds:KeyInfo Id="KeyId-18464534">
<wsse:KeyIdentifier
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentifier">u9LFn414C
6Fdpr1x875aHM6tVkk=
</wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
<wsse:Username>PESOT924</wsse:Username>
<wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">PASSWORD1</wsse:Password>
<wsse:Nonce>TKIX9rZyRHr6Ao5wJGgXjw==</wsse:Nonce><wsu:Created>2008-07-21T14:42:25.104Z</wsu:Created></wsse:UsernameToken>
</ds:Signature>
</soapenv:Body>
</soapenv:Envelope>
8.2.1.2 **PING Request SOAP Body**

The ping request must have no part defined and must have an empty `<soap:Body/>`.

**8.2.2 Response**

8.2.2.1 **Ping Operation Response**

The following are the response status codes for the ping operation:

<table>
<thead>
<tr>
<th>Element</th>
<th>Value</th>
<th>Element</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;statusCode&gt;</code></td>
<td>0000</td>
<td><code>&lt;statusDescription&gt;</code></td>
<td>Successful</td>
</tr>
<tr>
<td><code>&lt;statusCode&gt;</code></td>
<td>0151</td>
<td><code>&lt;statusDescription&gt;</code></td>
<td>System Failure</td>
</tr>
</tbody>
</table>

8.2.2.1.1 **PING SOAP Success Response**

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <ns1:ActionResponse xmlns:ns1="http://cbsv.ssa.gov/ws/datatype">
      <ns1:responseCode>0000</ns1:responseCode>
      <ns1:responseDescription>Successful</ns1:responseDescription>
    </ns1:ActionResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

8.2.2.2 **Failure Responses**

The following SOAP fault responses are returned if the request does not pass schema validation, or if the user is not authenticated or not authorized.

<table>
<thead>
<tr>
<th>SOAP Fault</th>
<th>Sample SOAP Body</th>
</tr>
</thead>
</table>
| Schema Validation Failure | `<env:Fault>
<faultCode>env:Server</faultCode>
<faultString>Schema validation failure</faultString>
</env:Fault>` |
| Authentication Failure | `<env:Fault>
<faultCode>env:Server</faultCode>
<faultString>Authentication Failure</faultString>
</env:Fault>` |
8.3 **VERIFY REQUEST AND RESPONSE STRUCTURE**

The `verify` operation compares the data provided by the Requesting Party with the data in the SSA master files. The Requesting Party’s credentials are used to authenticate the request.

### 8.3.1 Request

The following data elements will be sent in the SOAP header of the `verify` request:

<table>
<thead>
<tr>
<th>Element</th>
<th>Value Required?</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;wsse:SecurityTokenReference&gt;</code></td>
<td>Required</td>
<td>Value is the public key of the certificate</td>
<td>See example in Section 8.2.1.1</td>
</tr>
<tr>
<td><code>&lt;wsse:UsernameToken&gt;</code></td>
<td>Required</td>
<td>Includes eight-digit <code>&lt;Username&gt;</code> and <code>&lt;Password&gt;</code>; see example for child elements that may be required (such as Nonce, Created)</td>
<td>See example in Section 8.2.1.1</td>
</tr>
<tr>
<td><code>&lt;ds:Signature xmlns=&quot;http://www.w3.org/2000/09/xmldsig#&quot;&gt;</code></td>
<td>Required</td>
<td>See example for child elements that may be required</td>
<td>See example in Section 8.2.1.1</td>
</tr>
</tbody>
</table>
### Interface Specification for Consent Based SSN Verification Web Service

#### Element Specification

<table>
<thead>
<tr>
<th>Element</th>
<th>Value Required?</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ssn&gt;</td>
<td>Required</td>
<td>Nine-digit SSN</td>
<td>123456789</td>
</tr>
<tr>
<td>&lt;firstName&gt;</td>
<td>Required</td>
<td>Ten-character First Name</td>
<td>JOHN</td>
</tr>
<tr>
<td>&lt;middleName&gt;</td>
<td>Optional</td>
<td>Seven-character Middle Name</td>
<td>M</td>
</tr>
<tr>
<td>&lt;lastName&gt;</td>
<td>Required</td>
<td>Thirteen-character Last Name</td>
<td>SMITH</td>
</tr>
<tr>
<td>&lt;dateOfBirth&gt;</td>
<td>Optional</td>
<td>MMDDYYYY</td>
<td>07041974</td>
</tr>
<tr>
<td>&lt;genderCode&gt;</td>
<td>Optional</td>
<td>F or M</td>
<td>M</td>
</tr>
</tbody>
</table>

The `<Username>` tag contains the Requesting Party’s user ID, which is alpha-numeric and eight characters in length.

The `<Password>` tag contains the Requesting Party’s password. It must be eight characters in length, contain all uppercase letters, and be alpha-numeric.

The `<ssn>` tag contains an SSN. It must be nine digits long and within valid value ranges of SSNs issued by SSA.

The `<firstName>` tag contains a first name (no suffixes). It is a required element, and the maximum length allowed is 10 characters. It must contain only upper-case letters A to Z. Any other characters such as apostrophes, spaces, periods, and hyphens are removed, and the first name is compressed. If the first name exceeds 10 characters, the excess characters at the end of the first name are truncated. If the first name matches keywords restricted by SSA interface, a failure response is generated.*

The `<middleName>` tag contains a middle name (no suffixes). It is an optional element, and if it is included in the request, the maximum length allowed is seven characters. It must contain only upper-case letters A to Z. Any other characters such as apostrophes, spaces, periods, and hyphens are removed, and the middle name is compressed. If the middle name exceeds seven characters, the excess characters at the end of the middle name are truncated. If the middle name matches keywords restricted by SSA, a failure response is generated.*

---

* In such instances, the Requesting Party can use the CBSV online service for name/SSN verification as an alternative. It is recommended that the requesting party register for a CBSV online username and password at the time of registration for SSN verification service.
The `<lastName>` tag contains a last name (no suffixes). It is a required element, and the maximum length allowed is 13 characters. It must contain only upper-case letters A to Z. Any other characters such as apostrophes, extra spaces, periods, and hyphens are removed, and the last name is compressed. If the last name exceeds 13 characters, the excess characters at the end of the last name are truncated. If the last name matches keywords restricted by SSA, a failure response is generated.

The `<dateOfBirth>` tag contains the eight-digit string representing the month of birth in the format MM, day of birth in the format DD, and year of birth in the format YYYY (i.e., MMDDYYYY). It is an optional element. It is verified that the month (MM) is in the range of 01 to 12, the date (DD) is in the range of 01 to 31, the year (YYYY) is in the range of 1900 to “current year minus 12.” There shall be error handling and validation to avoid incongruous date information, e.g., April 31, Feb 29 on non-leap years, etc.

The `<genderCode>` tag contains the one-digit character F for Female or M for Male. It is an optional element.

### 8.3.1.1 VERIFY Request SOAP Header

See Section 8.2.1.1.

### 8.3.1.2 VERIFY Request SOAP Body

```xml
<soapenv:Body wsu:Id="id-7644051"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">

<dat:VerifyRequest>
    <dat:ssn>123456789</dat:ssn>
    <dat:firstName>JOHN</dat:firstName>
    <dat:lastName>SMITH</dat:lastName>
    <dat:dateOfBirth/>
</dat:VerifyRequest>
</soapenv:Body>
```
8.3.2 Response

8.3.2.1 Verify Operation Response

The following are the response status codes for the verify operation.

<table>
<thead>
<tr>
<th>Element</th>
<th>Value</th>
<th>Element</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;statusCode&gt;</td>
<td>0000</td>
<td>&lt;statusDescription&gt;</td>
<td>Successful</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>0001</td>
<td>&lt;statusDescription&gt;</td>
<td>Verification successful, but this person is deceased</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>9991</td>
<td>&lt;statusDescription&gt;</td>
<td>Verification unsuccessful</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>9910</td>
<td>&lt;statusDescription&gt;</td>
<td>Agreement in force: Negative account balance</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>9920</td>
<td>&lt;statusDescription&gt;</td>
<td>Agreement in force: No account found</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>9930</td>
<td>&lt;statusDescription&gt;</td>
<td>Agreement in force: Unable to check account balance</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>9940</td>
<td>&lt;statusDescription&gt;</td>
<td>Agreement not in force</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>9950</td>
<td>&lt;statusDescription&gt;</td>
<td>Agreement not in force: Negative account balance</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>9960</td>
<td>&lt;statusDescription&gt;</td>
<td>Agreement not in force: No account found</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>9970</td>
<td>&lt;statusDescription&gt;</td>
<td>Agreement not in force: Unable to check account balance</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>9980</td>
<td>&lt;statusDescription&gt;</td>
<td>No agreement found: Unable to check account balance</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>9990</td>
<td>&lt;statusDescription&gt;</td>
<td>Systems problem: API not functioning or network unavailable</td>
</tr>
<tr>
<td>&lt;statusCode&gt;</td>
<td>0151</td>
<td>&lt;statusDescription&gt;</td>
<td>System Failure</td>
</tr>
</tbody>
</table>

8.3.2.1.1 Verify Success SOAP Body

```xml
<ns1:responseCode>0000</ns1:responseCode>
<ns1:responseDescription>Verification Successful</ns1:responseDescription>
```
### 8.3.2.2 Failure Responses

The following SOAP fault responses are returned if the request does not pass schema validation or if the user is not authenticated or not authorized.

<table>
<thead>
<tr>
<th>SOAP Fault</th>
<th>Sample SOAP Body</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Schema Validation Failure</strong></td>
<td><code>&lt;env:Fault&gt;</code>&lt;br&gt;  &lt;faultcode&gt;env:Server&lt;/faultcode&gt;&lt;br&gt;  &lt;faultstring&gt;Schema validation failure&lt;/faultstring&gt; &lt;/env:Fault&gt;</td>
</tr>
<tr>
<td><strong>Authentication Failure</strong></td>
<td><code>&lt;env:Fault&gt;</code>&lt;br&gt;  &lt;faultcode&gt;env:Server&lt;/faultcode&gt;&lt;br&gt;  &lt;faultstring&gt;Authentication Failure&lt;/faultstring&gt; &lt;/env:Fault&gt;</td>
</tr>
<tr>
<td><strong>Authorization Failure</strong></td>
<td><code>&lt;env:Fault&gt;</code>&lt;br&gt;  &lt;faultcode&gt;env:Server&lt;/faultcode&gt;&lt;br&gt;  &lt;faultstring&gt;Authorization Failure&lt;/faultstring&gt; &lt;/env:Fault&gt;</td>
</tr>
<tr>
<td><strong>Verification Failure</strong></td>
<td><code>&lt;ns1:responseCode&gt;</code>9991<code>&lt;ns1:responseCode&gt;</code>&lt;br&gt;  &lt;ns1:responseDescription&gt;Verification unsuccessful&lt;/ns1:responseDescription&gt; &lt;/ns1:ActionResponse&gt;</td>
</tr>
</tbody>
</table>

Note: If the CBSV Web Service returns “Authentication Failure” response only for a particular name/SSN verification request, then that Web Service request may contain data that the SSA interface restricts as keywords. In such instances, the Requesting Party can use the CBSV online service for name/SSN verification as an alternative. It is recommended that the requesting party register for a CBSV online username and password at the time of registration for SSN verification service. For the online registration process, please refer to the CBSV User Guide available at [http://www.ssa.gov/cbsv/library.html](http://www.ssa.gov/cbsv/library.html)
9.0 WSDL AND XML SCHEMA DEFINITION

The most recent CBSV Web Service WSDL file is available at the following location: https://ws.ssa.gov/CBSVWS/services/CBSVServices?wsdl.

9.1 CBSV SERVICES-WSDL

```xml
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="http://www.ssa.gov/cbsv/
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/
xmlns:xsd="http://www.w3.org/2001/XMLSchema
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/
xmlns:tns="http://www.ssa.gov/cbsv/
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl
xmlns:impl="http://cbsv.ssa.gov/ws/datatype
xmlns="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:types>
    <xsd:schema>
      <xsd:import namespace="http://cbsv.ssa.gov/ws/datatype"
schemaLocation="CBSVServices.xsd"/>
    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="verifyRequest">
    <wsdl:part name="verifyRequest" element="impl:VerifyRequest">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="verifyResponse">
    <wsdl:part name="verifyResponse" element="impl:ActionResponse">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="pingResponse">
    <wsdl:part name="pingResponse" element="impl:ActionResponse">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="pingRequest">
  </wsdl:message>
  <wsdl:portType name="CBSVServicesPortType">
    <wsdl:operation name="ping">
      <wsdl:input message="tns:pingRequest" wsaw:Action="wsdl:ping">
      </wsdl:input>
      <wsdl:output message="tns:pingResponse">
      </wsdl:output>
    </wsdl:operation>
    <wsdl:operation name="verify">
      <wsdl:input message="tns:verifyRequest" wsaw:Action="wsdl:verify">
      </wsdl:input>
      <wsdl:output message="tns:verifyResponse">
      </wsdl:output>
    </wsdl:operation>
  </wsdl:portType>
</wsdl:definitions>
```
Interface Specification for Consent Based SSN Verification Web Service

<wSDL:binding name="CBSVServicesSoapBinding" type="tns:CBSVServicesPortType">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <wSDL:operation name="ping">
    <soap:operation soapAction="ping" style="document"/>
    <wSDL:input>
      <soap:body use="literal"/>
    </wSDL:input>
    <wSDL:output>
      <soap:body use="literal"/>
    </wSDL:output>
  </wSDL:operation>
  <wSDL:operation name="verify">
    <soap:operation soapAction="verify" style="document"/>
    <wSDL:input>
      <soap:body use="literal"/>
    </wSDL:input>
    <wSDL:output>
      <soap:body use="literal"/>
    </wSDL:output>
  </wSDL:operation>
</wSDL:binding>
<wSDL:service name="CBSVServices">
  <wSDL:port name="CBSVServicesPort" binding="tns:CBSVServicesSoapBinding">
    <soap:address location="http://localhost:9080/CBSVWebService/services/CBSVServices"/>
  </wSDL:port>
</wSDL:service>
</wSDL:definitions>

9.2 CBSVSERVICES-XSD

<?xml version="1.0" encoding="UTF-8"?>
<xSD:schema xmlns:xSD="http://www.w3.org/2001/XMLSchema"
  xmlns="http://cbsv.ssa.gov/ws/datatype"
  attributeFormDefault="qualified" elementFormDefault="qualified"
  targetNamespace="http://cbsv.ssa.gov/ws/datatype">
  <xSD:element name="ActionResponse">
    <xSD:complexType>
      <xSD:sequence>
        <xSD:element name="responseCode" type="xSD:string"/>
        <xSD:element name="responseDescription" type="xSD:string"/>
      </xSD:sequence>
    </xSD:complexType>
  </xSD:element>
  <xSD:element name="VerifyRequest">
    <xSD:complexType>
      <xSD:sequence>
        <xSD:element name="ssn" type="xSD:string"/>
      </xSD:sequence>
    </xSD:complexType>
  </xSD:element>
</xSD:schema>
Interface Specification for Consent Based SSN Verification Web Service

<xsd:schema>
  <xsd:element name="firstName">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="10"/>
        <xsd:minLength value="1"/>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>

  <xsd:element name="middleName" nillable="true">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="7"/>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>

  <xsd:element name="lastName">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="13"/>
        <xsd:minLength value="1"/>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>

  <xsd:element name="dateOfBirth" nillable="true">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:pattern value="^\d{4}\d{2}\d{2}$/">
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>

  <xsd:element name="genderCode" nillable="true">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:pattern value="[mfMF]?"/>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
</xsd:sequence>
</xsd:complexType>
</xsd:schema>
10.0 ACRONYMS

The following list defines the acronyms used throughout this document.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Acronym Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>BSO</td>
<td>Business Services Online</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CBSV</td>
<td>Consent Based SSN Verification Project</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IRES</td>
<td>Integrated Registration Services</td>
</tr>
<tr>
<td>SSA</td>
<td>Social Security Administration</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>SSN</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>User ID</td>
<td>User Identifier</td>
</tr>
<tr>
<td>W3C</td>
<td>World Wide Web Consortium</td>
</tr>
<tr>
<td>WSDL</td>
<td>Web Services Description Language</td>
</tr>
<tr>
<td>WSS</td>
<td>Web Services Security</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
<tr>
<td>XSD</td>
<td>XML Schema Definition</td>
</tr>
</tbody>
</table>