CBSV WEB SERVICE CLIENT DEVELOPMENT REFERENCE GUIDE

4/3/2014 10:55 AM

TABLE OF CONTENTS

1.0 INTRODUCTION

Consent Based Social Security number (SSN) Verification (CBSV) is a fee and consent-based SSN verification service provided by Social Security Administration (SSA) to enrolled private businesses, hereafter referred to as Requesting Parties. This service provides real-time SSN verifications with the capability of handling a small to large volume of requests. Using CBSV, Requesting Parties can verify whether the identity information obtained from a consenting Number Holder matches the data in SSA's records. CBSV application verifies the following submitted identity information against SSA's Master File of SSNs:

- SSN
- First Name
- Middle Name (optional)
- Last Name
- Suffix (optional, and only verified through CBSV Online)
- Date of Birth

1.1 OVERVIEW OF CBSV SERVICE

CBSV provides two service channels for SSN verification:

- Web Service
- Online

1.2 PURPOSE OF THE DOCUMENT

The purpose of this document is to focus on the basic technical knowledge, programming skills, and software requirements to develop the CBSV Web Service Client application. This document serves as a guide for new Requesting Parties to assess their current technical proficiency, provides guidance to develop Web Service client software, and to conduct interface testing with CBSV Web Service.

The document is organized into the following sections:

- Section 1- Introduction: provides an overview of the CBSV service, and the purpose of this document.
- Section 2- CBSV Web Service Client Development Requirements: presents a high-level description of the technical expertise and security requirements to develop the CBSV Web Service Client application.
- Section 3- SSA Recommended technologies: presents a high-level description of the technologies used by SSA to develop client code to test the CBSV Web Service.

- Section 4- Testing: provides a description of the SSA Test environment, and SSA recommended testing tools.
- Section 5- Helpdesk Support: provides information about SSA's customer support operations.
- Section 6- References: lists hyperlinks to CBSV service resources, for reference.
- Section 7- Appendix: provides information on X.509 Digital Certificates and answers to commonly asked questions about CBSV Web Service.
- Section 8- Acronyms: lists the acronyms used throughout this document.

2.0 CBSV WEB SERVICE CLIENT DEVELOPMENT REQUIREMENTS

CBSV Web Service conforms to the World Wide Web Consortium (W3C) Web service standards (SOAP, Web Service Definition Language [WSDL], and Web Service Security [WSS]). SSA has successfully tested the CBSV Web Service with client code developed in Java and C# (Microsoft .Net Framework) based industry standard technologies; and recommends these technologies to the Requesting Parties for developing their client application. However, a Requesting Party can develop CBSV Web Service client application in any technology that supports the same Web Service standards as CBSV Web Service.

2.1 GENERAL TECHNICAL COMPETENCIES

In order to develop CBSV Web Service Client software independently, the development team of the Requesting Parties must have thorough understanding and expertise in the following technical areas:

- WSDL
- SOAP
- WSS
- Transport layer security using Hypertext Transfer Protocol Secure (HTTPS)
- Extensible Markup Language (XML)
- XML Data Creation, Data Parsing, Schema
- Secure Socket Layer (SSL) Digital Certificates using X.509 Standards

2.2 CBSV WEB SERVICE SECURITY

To implement security for the data exchanged between the CBSV Web Service and its clients, CBSV Web Service uses the following techniques:

- User Authentication: The Requesting Party's authorized representative must register with SSA, and get a User Identifier (ID)/password (Credential), as well as acquire access to CBSV Web Service. More details can be found in the CBSV User Guide located at http://www.ssa.gov/cbsv/docs/CBSVInterfaceSpecification.pdf .
- HTTPS: CBSV Web Service secures the communication with the Client application using HTTPS, ensuring proper encryption of the data exchanged.
- Digital Signature: The SOAP message sent by a CBSV Web Service client must include the X.509 digital certificate issued by a trusted Certificate Authority (CA). Refer to Section 7.0 on the process required for obtaining a Digital Certificate by a Requesting Party.

CBSV Web Service client must utilize the SOAP for message packaging and implement the WSS to include the credential and the Digital Signature in the SOAP message sent to CBSV Web Service.

2.3 CBSV WEB SERVICE CLIENT DEVELOPMENT

Requesting Parties need to develop Web Service Client application based on the CBSV Web Service WSDL. SSA strongly recommends Requesting Parties who are considering using CBSV Web Service to evaluate the available standard technologies for development of the client software.

The client application must be able to perform the following functions:

- Collect the SSN Holder's identity data as input
- Include a data structure (for input data that needs to be verified), which is acceptable by CBSV Web Service as described by the WSDL
- Include a digital certificate and use its private key with the key identifier type set to "*Subject Key Identifier*" to sign the request SOAP message conforming to the specification of WSS
- Include the Credential of the registered representative in the SOAP message with the password type set to "*PasswordText,*" conforming to the specification of WSS
- Create the SOAP message which adheres to the specifications as outlined in SOAP version 1.2

  Note: Strong authentication employing the Credential and the digital signature is required to access CBSV Web Service successfully.
- Connect to CBSV Web Service using HTTPS to perform the SSL handshake successfully
- Send the request SOAP message
- Receive and parse the response from CBSV Web Service to retrieve results
- Incorporate Client side error handling as needed. (Optional)

Note: Client side error handling is not required for the Web Service client to interface with CBSV Web Service.

3.0 SSA RECOMMENDED TECHNOLOGIES

3.1 JAVA

In order to develop the Java based CBSV Web Service client application, SSA recommends the following technical requisites:

- **Oracle Java Development Kit (JDK, Version 1.5 or higher)**
- **Application development using Java 2 Enterprise Edition (J2EE)**
- **A J2EE Application Server (IBM WebSphere Application Server, JBOSS, BEA WebLogic, etc.)**
- **Java key store management (keytool)**: Manages a key store (database) of private keys and their associated X.509 certificate chains authenticating the corresponding public keys, as well as manages certificates from trusted entities
- **Java based WS Engine (JAX-RPC/JAX-WS/Apache Axis2)**: Usage of WS engine to perform client development based on Web Service WSDL
- **WS-Security Java implementation:** Rampart or equivalent

3.2 .NET

In order to develop the C# (Microsoft .Net Framework) based CBSV Web Service client, SSA recommends the following technical requisites:

- **Microsoft Visual Studio:** Microsoft Visual Studio 2010 or higher is an Integrated Development Environment (IDE) and can be used to develop Web applications and Web Services in C# programming language supported by .NET framework
- **.NET Framework 4.0 Software Development Kit (SDK):** .NET Framework 4.0 SDK or higher enables developers to build secure Web Services based on the latest Web Services protocol specifications
- **Microsoft Management Console (MMC) 3.0 framework SDK**: MMC 3.0 or higher is a framework that hosts administrative tools, called snap-ins, on Windows operating systems. Administrators can use MMC to administer networks, computers, services, and other system components. MMC can be used to store the X.509 certificate to a trusted store.
- **Certificate Creation Tool** (**Makecert.exe)**: This tool generates X.509 certificates that you may use for testing purposes only. It creates a public and private key pair for digital signatures and stores them in a certificate file. This SDK tool comes with the installation of the .NET Framework SDK
- **.NET Framework Namespaces:** Microsoft.Web.Services3 is the set of core classes used for Microsoft .NET WSE-enabled applications and System.NET.Security Namespace provides network streams for secure communications between hosts

- **Web Services Enhancements (WSE) 3.0:** WSE 3.0 or higher for .NET framework is an add-on to Microsoft Visual Studio 2005 and should be separately downloaded for Microsoft Visual Studio 2010, which allows adding message-level security to Web Service applications.

4.0 TESTING

4.1 TEST ENVIRONMENT

SSA provides a test environment for CBSV Web Service so that CBSV Web Service clients in development can connect to this test environment and perform Interface testing of their software with CBSV Web Service. SSA recommends that the Requesting Parties set up and configure an independent test environment to connect to SSA's testing environment. The test environment must be implemented to replicate the Production environment, including network connectivity, network security, WSS, and SSN Verifications to ensure proper handling of the responses returned to the client software.

4.2 REQUIREMENTS

The Requesting Party must meet the following requirements to conduct secure SOAP message exchanges with the CBSV Web Service during Interface Testing:

4.2.1 PROCEDURAL REQUIREMENTS

- **User Agreement**: SSA requires Requesting Parties to sign a User Agreement in order to be eligible to access SSA's Test environment. Per SSA policies, Requesting Parties' acceptance to all the terms and conditions of the User Agreement is required before Interface testing with CBSV Web Service is permitted.
- **Time Allocation**: The Requesting Party can conduct Interface testing with CBSV Web Service for a specified period, as allocated by SSA. The Requesting Party must contact SSA in advance to schedule additional time, if needed.

4.2.2 TECHNICAL REQUIREMENTS

- **Digital Certificates**: To ensure strong authentication, Requesting Parties must provide a X.509 digital certificate public key that will be used to sign the request SOAP message. The certificate can be acquired from a recognized, trusted Certification Authority (CA) or a self-signed certificate may be submitted to SSA for test purposes only.

Note: Since a self-signed certificate is created and signed by the Requested Party itself and is not attested from a trusted CA or evaluated for validity, it is implied that the Requesting Party also signed off on its legitimacy. The Requesting Party must e-mail the ".cer" file that contains the public key for their X.509 certificate to SSA at ACUT@ssa.gov.

4.2.3 TEST DATA

SSA provides Test Data that generates response messages in the Test environment to replicate messages generated by the CBSV Web Service in the Production environment. Each test scenario typically verifies that a given set of input produces expected results. The Test environment will not contain the Agreement and Finance verifications. It involves testing with pre-defined Test Data input with checks including: access and connectivity, SSN Verification generates a unique response code, and the response description and proper fault response in case of failures.

To request additional testing details or test data, send e-mails to OSES.ETE.Support.Mailbox@ssa.gov.

The following table lists the code and description of the response messages generated by CBSV Web Service:

Response Generated by	Response Code	Response Message	Description
Ping operation	0000	**Successful**	CBSV Web Service is running and is available
Ping operation	0151	**System Failure**	CBSV Web Service is down and not available to process incoming request message
Verify operation	0000	**Verification Successful**	SSN Test data verified successfully and is valid
Verify operation	0001	**Verification Successful, but deceased**	SSN Test data verified successfully, but the SSN holder is deceased
Verify operation	9991	**Verification unsuccessful**	SSN Test data verified successfully and is invalid
Verify operation	0151	**System Failure**	Input data is invalid and system unable to convert data into the compatible format

Response Generated by	Response Code	Response Message	Description
Verify operation	9900	**This is a verification for a minor. For these verifications, the request must contain a 'Y' in the 'minor' field attesting that the proper authorization for the minor SSN holder was obtained. You may not verify the SSN of a minor without this authorization.**	The minor date of birth requires a 'Y' in the 'minor' field in the Web Service request.
Verify operation	9910	**Agreement in force: Negative account balance**	It is determined that a valid agreement exists, but there is a negative account balance.
Verify operation	9920	**Agreement in force: No account found**	It is determined that a valid agreement exists, but a financial account does not exist.
Verify operation	9930	**Agreement in force: Unable to check account balance**	It is determined that a valid agreement exists, but the system is unable to confirm the requesting party's account balance.
Verify operation	9940	**Agreement not in force**	It is determined that the agreement is not in force.
Verify operation	9950	**Agreement not in force: Negative account balance**	It is determined that the agreement is not in force, and there is a negative account balance.
Verify operation	9960	**Agreement not in force: No account found**	It is determined that the agreement is not in force, and a financial account does not exist.
Verify operation	9970	**Agreement not in force: Unable to check account balance**	It is determined that the agreement is not in force, and the system is unable to check the account balance.

Response Generated by	Response Code	Response Message	Description
Verify operation	9980	**No agreement found: Unable to check account balance**	It is determined that an agreement does not exist, and the system is unable to confirm the account balance.
Verify operation	9990	**Systems problem: API not functioning or network unavailable**	System or network is unavailable.
Security Check		**Authentication Failure**	It is determined that user's credentials <userid> and/or <password> could not be authenticated, possibly due to invalid credentials, password expiration, or client Digital Certificate is invalid.
Security Check		**Authorization Failure**	It is determined that the user's credential is not authorized to access the CBWS Web Service application.
Security Check		**Schema Validation Failure**	Input SOAP message could not be validated against CBSV Web Service WSDL file and schema specifications.
Security Check	0151	**System Failure**	CBSV Web Service is down and not available to process incoming request message

Note: If the Requesting Party receives response or failure not listed in this table, the Requesting Party must examine its client software code to diagnose problems and identify errors before reporting issues to SSA.

4.2.4 TESTING TOOL

SoapUI is an Open Source Functional Testing Tool, mainly used for Web Service testing. It can generate a CBSV Web Service client based on CBSV Web Service WSDL file and can communicate securely with SSA using test data. It is useful to test the setup and configuration of network connectivity and WSS, including the validity of registered Credential.

5.0 HELPDESK SUPPORT

5.1 CBSV CUSTOMER SUPPORT

The CBSV customer support is available via telephone and e-mail. Customers can speak with a representative by calling 1-888-772-2970 during the following hours:

Day	**Time (***displayed in Eastern Standard Time***)**
Monday – Friday	8:30 a.m. to 4:00 p.m.

E-mail CBSV program specific inquiries to ssa.cbsv@ssa.gov.

For CBSV Web Service specific technical queries and Production issues, e-mail web.service.testing@ssa.gov.

CBSV is not available when SSA is in the process of implementing changes to systems. Whenever possible, SSA will post advance notices of outages on the SSA Business Services Online (BSO) Web site and CBSV Web site. SSA also notifies CBSV Web Service users about known outages via e-mail. If users attempt to use the CBSV Web Service while the system is unavailable, they will receive a failure response.

5.2 CBSV WEB SERVICE TEST ENVIRONMENT CUSTOMER SUPPORT

Test environment Customer support is available via e-mail during the following hours to troubleshoot issues experienced during CBSV Web Service Interface testing:

Day	**Time (***displayed in Eastern Standard Time***)**
Monday – Friday	8:30 a.m. to 4:00 p.m.

Send e-mails to OSES.ETE.Support.Mailbox@ssa.gov.

6.0 REFERENCES

6.1 REGISTRATION PROCESS

For information about the CBSV registration process, refer to the CBSV User Guide, available at http://www.ssa.gov/cbsv/docs/CBSVUserGuide.pdf.

6.2 CBSV WEB SERVICE WSDL

The CBSV Web Service WSDL document, which defines the list of the services provided and the interface required for each service offered for SSN verification, is available at https://ws.ssa.gov/CBSVWS/services/CBSVServices?wsdl. CBSV Web Service uses WSDL version 1.1 and SOAP version 1.2.

6.3 INTERFACE SPECIFICATION

The Interface Specification for CBSV Web Service, which provides interface requirements and operations, is available at http://www.ssa.gov/cbsv/webservice.html .

7.0 APPENDIX

7.1 X.509 DIGITAL CERTIFICATES

Following are the high-level steps required to obtain a X.509 Digital Certificate:

- Purchase a digital certificate from a trusted CA
- Send the public key of the digital certificate to SSA
- Obtain SSA's public key as a certificate
- Manage Key Store, that includes:
  - Key store creation
  - Importing the client's own private key to the key store
  - Importing the public key (of SSA), to the key store

7.2 FREQUENTLY ASKED QUESTIONS

Following are the answers to commonly asked questions about CBSV Web Service and developing the Web Service Client application:

1. **What is the system availability for CBSV Web Service in Production?**

   The CBSV service in Production is available to accept and process requests for SSN verifications during the following hours:

Day	**Time (***displayed in Eastern Standard Time***)**
Monday – Friday	5:00 a.m. to 1:00 a.m.
Saturday	5:00 a.m. to 11:00 p.m.
Sunday	8:00 a.m. to 11:30 p.m.

   CBSV service may not be available during planned outages or emergency maintenance. For more information on planned outages, contact web.services.testing@ssa.gov.

2. **What is the Contact information for CBSV Technical Support?**

   Technical support is available by e-mail at web.services.testing@ssa.gov. Or if you are having problems connecting, customers can speak with a representative Monday through Friday from 8:30 a.m. to 4:00 p.m., Eastern Time, by calling 1-888-772-2970.

3. **What technologies does SSA recommend for Web Service Client development?**

   SSA highly recommends that Requesting Parties develop their Web Service Client Software using Java and C# (Microsoft .Net) based technologies. SSA does not provide any support for

Web Service Clients developed using other technologies such as Hypertext Preprocessor (PHP) or Active Server Pages (ASP), etc.

4. **What version of WSDL and SOAP does CBSV Web Service use?**

   CBSV Web Service uses WSDL version 1.1 and SOAP version 1.2.

5. **What assistance does SSA provide?**

   SSA provides assistance with connectivity issues experienced while accessing CBSV Web Service during Interface Testing and in Production. Common connectivity issues are "Authentication Failure", and "Authorization failure". SSA provides limited Web Service Client application specific support. The intent of this support is to help with CBSV Web Service Client development, establish connectivity, and verify that SSA's environment is operational – not to troubleshoot the Requesting Party's application specific errors.

6. **What is the CBSV Web Service Production endpoint?**

   The CBSV Web Service WSDL file in Production is available at the following location: https://ws.ssa.gov/CBSVWS/services/CBSVServices?wsdl. This WSDL file specifies the requirements for providing and consuming the CBSV Web Service. It acts as a contract and populates the Ping and Verify operation signatures of the CBSV Web Service.

7. **How can the Requesting Party check the CBSV Web Service availability in the Test environment?**

   The CBSV Web Service WSDL file in the SSA Test environment is available at https://etews.ssa.gov/CBSVWS/services/CBSVServices?wsdl. This hyperlink displays the CBSV Web Service WSDL file as defined in the Interface Specification document located at http://www.ssa.gov/cbsv/docs/CBSVInterfaceSpecification.pdf. If the WSDL file is not accessible, an e-mail may be sent to OSES.ETE.Support.Mailbox@ssa.gov. Testing cannot be conducted without prior notification and receipt of active test data.

8. **What is an Authentication Failure?**

   Following are the common reasons for Authentication Failure:

   - If the associated Credential is:
     - Invalid: Incorrect value of the User ID and/or password
     - Expired password: To prevent password expiration, it is mandatory to change the CBSV Web Service password in accordance with SSA's password policies. The user will not be prompted to change the password when using the CBSV Web Service.

   For detailed information on password requirements, please refer to the CBSV User Guide, available at http://www.ssa.gov/cbsv/docs/CBSVUserGuide.pdf. Maintain a valid public key to SSA: If the Requesting Party does not provide a valid public key of their Digital Certificate.

   - Valid SOAP message: The encrypted request SOAP message does not include valid digital signatures in compliance with X.509 standards.

9. What is an Authorization Failure?

CBSV Web Service returns an "Authorization failure" response if the User ID used to connect with CBSV Web Service is not associated with the appropriate CBSV Web Service role.

10. What are the requirements for performing CBSV Web Service Interface Testing?

- The Requesting Party must be able to meet SSA's schedule and perform testing during the agreed upon timeframe with support available Monday through Friday between 8:30 a.m. and 4:30 p.m. Eastern Standard Time (EST).
- The Requesting party must provide SSA with the public key of the digital certificate.
- SSA will provide the Requesting Party with pre-defined test data to process various response messages, when required.
- SSA recommends that the Requesting Party have technical team members available to work with the SSA technical team to troubleshoot and resolve any connectivity or compatibility challenges incurred during the testing process.

11. What are the requirements to access CBSV Web Service in the Production environment?

CBSV Web Service secures communication and transactions conducted with the CBSV Web Service client applications, by enabling security over the transport layer using the HTTPS employing SSL certificates signed by a well-known, trusted Certification Authority (CA). Strong authentication is ensured using X.509 client certificates, which authenticates the Requesting Party, based on a digital signature over the SOAP: body element.

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 of this certificate.

The Requesting Party must e-mail the ".cer" file that contains the public key for the X.509 certificate to SSA at ACUT@ssa.gov. The .cer extension of the certificate must be changed to .txt before sending. The file can also be e-mailed using compression software with a ".zip" extension.

12. How to update the CBSV Web Service associated credential password?

The password can be updated by logging into SSA's Business Services Online (BSO) application at http://www.ssa.gov/bso/bsowelcome.htm.

Note: The System will not prompt users to change passwords when using the CBSV Web Service.

13. Why does SSN Verification data receive a failure response in Production?

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. For more details, send e-mail to web.service.testing@ssa.gov.

Note: In such instances, the Requesting Party can use the CBSV Online service for name/SSN/date of birth verification. SSA requires a separate User ID for CBSV Online.

14. Who can issue SSL Certificates?

The SSL Certificate must be issued by a "Trusted Certifying Authority" (trusted third party Certification Authorities that utilize their trusted position to make available "trusted" SSL Certificates).

15. What is a Trusted Certification Authority?

CA is an entity that issues digital certificates. Standard Browsers and Operating Systems come with a pre-installed list of trusted Certification Authorities, known as the Trusted Root CA store. SSL certificates issued by trusted Certification Authorities do not display a warning and establish a secure link between Web site and browser transparently. Because of their "trusted" status, Certification Authorities have a responsibility to ensure they only issue SSL Certificates to legitimate companies.

8.0 ACRONYMS

The following list defines the acronyms used throughout this document.

Acronym	Acronym Definition
CBSV	Consent Based Social Security Number Verification
CA	Certification Authority
HTTPS	Hypertext Transfer Protocol Secure
IDE	Integrated Development Environment
JDK	Java Development Kit
MMC	Microsoft Management Console
SDK	Software Development Kit
SSA	Social Security Administration
SSL	Secure Socket Layer
SSN	Social Security Number
User ID	User Identifier (issued by SSA)
URL	Uniform Resource Locator
WSDL	Web Services Description Language
WSE	Web Services Enhancements
WSS	Web Service Security
W3C	World Wide Web Consortium
XML	Extensible Markup Language