Traveler Verification Service

(Cloud-Based Matching)

Technical Reference Guide – Authentication API

U.S. Customs and Border Protection

March 2019

Version 1.9

Change Control Log

Revised By	Revised Version Number	Date	Description of Revisions
CBP OIT	V1.0	02/15/2017	Initial Document
CBP OIT	V1.1	03/21/2017	1. Convert the Swagger API details and screenshot to URL references 2. Updated document format 3. Sample request/response messages 4. New section: Connectivity/Networking
CBP OIT	V1.2	05/04/2017	1. Update API URL 2. Update UTC time details
CBP OIT	V1.3	05/10/2017	1. Added Section on Authorization Header (3.1.4) 2. Revised the Response for Identify API 3. Revised Disposition for Token and deviceId under Identify Message Elements (3.2.2)
CBP OIT	V1.4	05/17/2017	1. Specifying the use of Operating Carrier Code and Operating Flight Number (3.2.1) 2. Specifying the use of Operating Carrier Code and Operating Flight Number (3.2.2)
CBP OIT	V1.5	05/23/2018	1. Addition of Details for Cruise Vessels
CBP OIT	V1.6	07/20/2018	1. Revised Table in Section 3.2.3 to Modify Token from Mandatory to Optional
CBP OIT	V1.7	09/18/2018	1. Revised the Introduction, Internet Connectivity, and TVS Environments Sections (1,3,5) 2. Added a Section on Project Plan (2) 3. Added Section on Authorization Errors (3.2) 4. Separated out the Identify API into its own Technical Reference Guide
CBP OIT	V1.8	01/11/2019	1. Revised Network Connection Test (Section 3.3) 2. Updated the Requirements for Login and Refresh Token APIs, Sections (4.1.3, 4.2)

Revised By	Revised Version Number	Date	Description of Revisions
			3. Updated the Minimum Password Length Section (4.3.1)
CBP OIT	V1.9	03/22/2019	1. Updated API Message Element Tables (Section 4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.3.2) 2. Updated Authentication Service Errors (Section 4.4)

Table of Contents

Table of Figures

1. Introduction

1.1 Background

U.S. Customs and Border Protection (CBP) is transforming the way it identifies and verifies travelers by shifting the key to unlocking the passenger profile from biographic to biometric identifiers. The CBP Office of Field Operations (OFO) has developed a comprehensive strategy to implement a biometric entry-exit solution for travelers departing by air, land, and sea as well as to provide enhancements for existing biometric entry capabilities. This strategy addresses the operational requirements aligned with capabilities to enhance CBP's ability to execute its border security mission:

- **Verify Traveler Identity**: The ability to capture, review, analyze, search, and match travelers' biometric information with Government biometric and biographic records when entering and exiting the U.S. for the purposes of verifying identity
- **Create and Manage Biometric Records**: The ability to record, store, and disseminate biometric information and metadata collected from non-U.S. citizen travelers entering and exiting the U.S.
- **Generate Metrics and Reports**: The ability to measure and report the effectiveness of the biometric entry-exit system

In 2016, CBP's Office of Information and Technology (OIT) concluded the initial phases of a facial recognition feasibility study. Facial recognition was chosen as the primary biometric verification modality based upon operational viability, availability of existing traveler photos, and successful feasibility studies utilizing facial recognition. The Traveler Verification Service (TVS) is the next transitional step towards deployment of reliable and repeatable biometric verification capabilities in the Air Exit/Entry, Sea Exit/Entry, and Land environments.

1.2 Overview and Purpose

CBP provides a TVS Web Service for external stakeholders to use for submission of traveler photos through an internet facing Application Program Interface (API) Gateway: Biometric Gateway API. The Biometric Gateway API provides a set of services to allow authenticated users the ability to perform biometric verification operations with CBP. There are two primary services involved: Authentication and Identify. The purpose of this document is to provide the interface specifications for the Authentication API between TVS and external stakeholders for various modalities within the CBP external environment. This document will be used in conjunction with the Technical Reference Guide for the Identify API, provided separately. CBP OIT will work closely with each stakeholder in developing, testing, and implementing the software.

1.3 Scope

The scope of this document covers the following modalities within the CBP external environment:

- Air Exit – Biometric verification of travelers exiting the U.S. at outbound international departure gates
- Transportation Security Administration (TSA) – Biometric verification of international travelers at TSA Checkpoints
- Sea Entry – Biometric verification of travelers entering the U.S. at sea ports
- Tokenless Identify – Non-Department of Homeland Security (CBP and TSA) confirmations and/or enforcement related biometric verification of traveler identities in support of a "Seamless Traveler Experience" such as in the following areas: boarding (foreign inbound), check in, baggage drop, and other approved uses.

2. Project Planning

All projects start with initiating an engagement and committing to implementing a biometric verification process. Generally, each project takes the following steps from initiation to implementation.

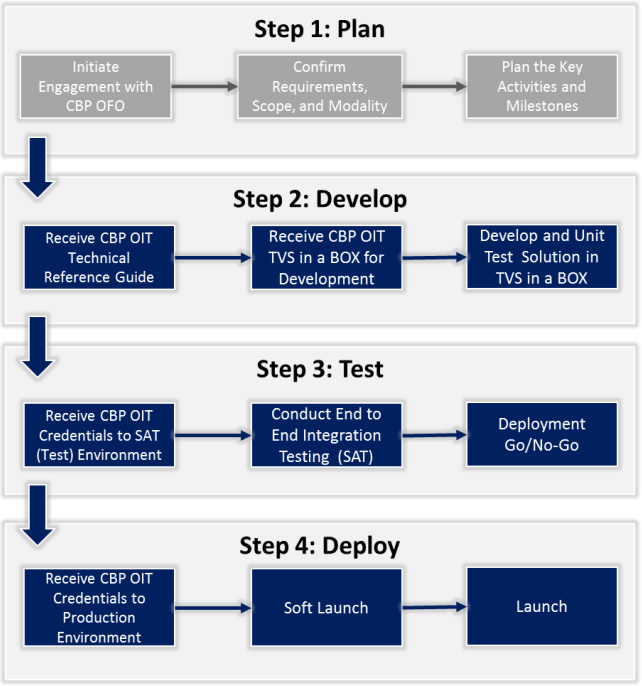

Figure 1: TVS Project Plan

2.1 Step 1: Plan

The objective of the planning step is to initiate engagement with CBP, lay out a path forward, and identify the points of contact (POCs). CBP and stakeholders will collaboratively define, document, and reach a consensus on the project requirements, scope, and modalities. These technical reference documents serve as the blueprints for development activities. A vital output from the planning step is a schedule that includes dates for development, testing, deployment, and launch.

2.2 Step 2: Develop

TVS comprises web services and a gateway to submit photos through an internet API. In the Development Step, stakeholders are expected to build and deploy the APIs needed to interface with TVS. CBP OIT will provide this TVS Technical Reference Guide that includes the technical specifications for the APIs, as well as the specifications for providing a facial recognition quality photo. CBP OIT will also provide an environment referred to as "TVS in a Box," which is a dedicated virtual instance intended to allow flexible development and unit testing. CBP OIT also provides technical support to assure proper guidance and resources are available when developing and testing the APIs.

2.3 Step 3: Test

Upon completion of development activities, preparation for deployment will begin by conducting joint end-to-end integration. The intent of this testing is to use the safe test environment to simulate operations, and identify and resolve any problems before moving into production. CBP OIT will provide access to the CBP System Acceptance Test (SAT) environment and available time slots for testing. CBP OIT will provide services needed to simulate options by generating the galleries, ingesting photos into the galleries, matching photos, and sending match responses. Upon completion of testing and resolution of any identified issues, a joint "Go" or "No Go" decision will be held, which will include revisions to the schedule as necessary.

2.4 Step 4: Deploy

Upon successful completion of the Test Step, the solution is ready for deployment. CBP OIT will provide access to the production environment. Once configured, the solution is ready for launch.

3. Internet Connectivity

3.1 Networking

The TVS API will be publicly available through the internet, upon successful secure authentication. It will not require calling systems to connect to CBP, DHS, or other U.S. government internal networks.

3.1.1 **HTTPS**: TVS will only be accessible via HTTPS. The service will present a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) certificate for the domain name that will need to be trusted by calling computer systems. CBP policy supports TLS 1.2.

3.1.2 **Virtual Private Network (VPN) Usage**: CBP does not support connection to TVS over a VPN.

3.2 Network Connection Speed Requirements

Reliable, high-speed internet access is required. High-speed is defined as having minimum network connection download speeds of 20 Mbps and upload speeds of 8 Mbps.

3.2.1 **Hardwired vs Wireless Connection**: A hardwired connection is preferred, but high-speed wireless will be adequate if the connection is reliable.

3.3 Network Connection Test

Provided below is a sample curl script that can be used to test the network connection.

Sample curl script with statistics

Curl Script:

```
curl -w '\nLookup time:\t%{time_namelookup}\nConnect time:\t%{time_connect}\nPreXfer
time:\t%{time_pretransfer}\nStartXfer time:\t%{time_starttransfer}\n\nTotal
time:\t%{time_total}\n' -o /devnull  -d '{"Username":"<valid username>", "Password":"<valid
password>"}' https://sat.tvs-cbp.com/api/auth/login
```

Curl Script Response:

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3584  100  3494  100    90   1486     38  0:00:02  0:00:02 --:--:--  1488

Lookup time:    0.002895
Connect time:   0.071676
PreXfer time:   0.696206
StartXfer time: 2.350225

Total time:     2.350514
```

Figure 2: Sample Curl Script Test Response

4. Authentication Service

The Authentication Service is a cloud service that allows the authentication of users. The diagram below illustrates the high-level architecture design for the Authentication Service. Included in the services are Login, Refresh Token, and Change Password.

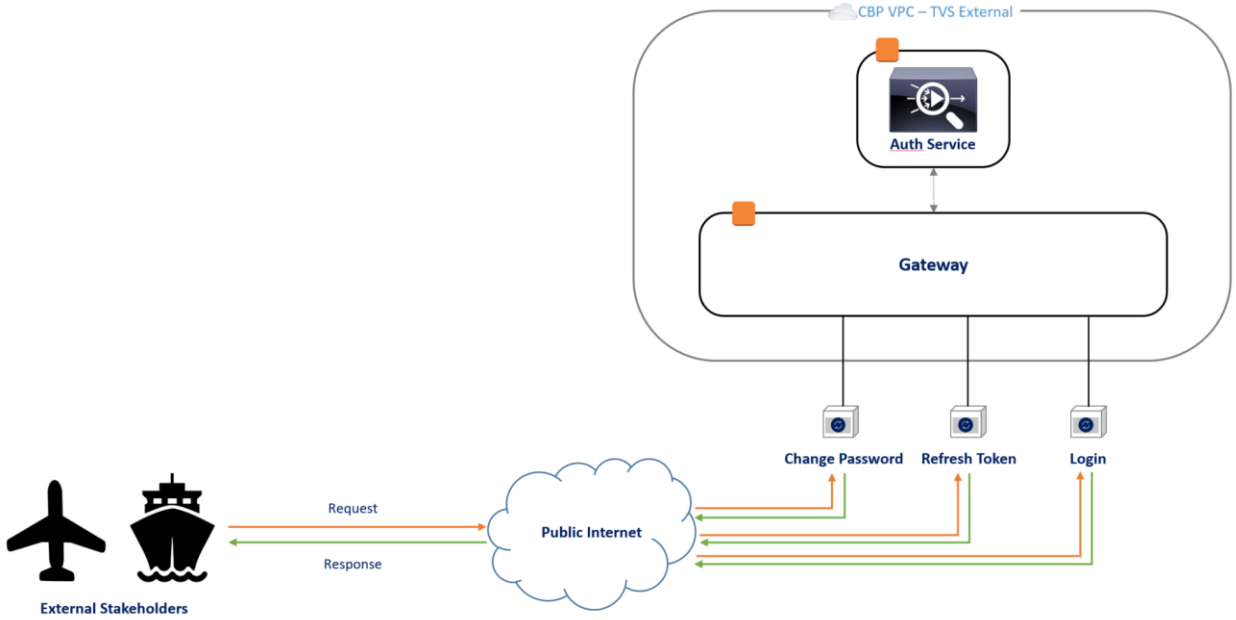

Figure 3: TVS Cloud-Based Authentication Service

4.1 Login API

The login API allows a user to authenticate to the system with a valid username and password. CBP will set up and provide a username and password for access.

Reference URL: https://tvs-cbp.com/api/auth/login
HTTP Method: POST

Message Direction	Format	Body Example
Request	JSON	`{ "Username": "USERNAME", "Password": "PASSWORD" }`
Response	JSON	`{ "AccessToken": "ACCESS TOKEN", "ExpiresIn": 3600, "TokenType": "Bearer", "RefreshToken": "REFRESH TOKEN", "IdToken": "ID TOKEN" }`

4.1.1 Login Request Message Elements

Data Element Name	Format	Disposition	Comment
Username	String	Mandatory	Username used for login
Password	String	Mandatory	Password used for login

4.1.2 Login Response Message Elements

Data Element Name	Format	Disposition	Comment
AccessToken	String	Mandatory	Grants access to authorized resources
ExpiresIn	Number	Mandatory	Token expires in 3600s
TokenType	String	Mandatory	Bearer
RefreshToken	String	Mandatory	Used in refreshToken API
IdToken	String	Mandatory	Used in the Authorization Header that identifies a user

4.1.3 **Login Considerations**: The following are important considerations when using the Login API:

- The IdToken will be used in the Authorization Header for subsequent API calls
- Login shall not be called every time before calling another API. Instead, call Login once and use the same IdToken for subsequent API calls
- The IdToken will expire after an hour, after which the refreshToken API should be called

4.2 Refresh Token API

During an active session, when the IdToken expires, the refreshToken API allows the user to refresh their IdToken in order to extend their authenticated session. The IdToken will be valid for 3,600 seconds (1 hour) after it has been refreshed. The user shall invoke the refreshToken API prior to the IdToken expiring to keep alive the active session.

Reference URL: https://tvs-cbp.com/api/auth/refreshToken
HTTP Method: POST

Message Direction	Format	Body Example
Request	JSON	`{ "RefreshToken": "REFRESH TOKEN" }`
Response	JSON	`{ "AccessToken": "ACCESS TOKEN", "ExpiresIn": 3600, "TokenType": "Bearer", "IdToken": "ID TOKEN" }`

4.2.1 Refresh Token Request Message Elements

Data Element Name	Format	Disposition	Comment
RefreshToken	String	Mandatory	Enter RefreshToken acquired from Login API

4.2.2 Refresh Token Response Message Elements

Data Element Name	Format	Disposition	Comment
AccessToken	String	Mandatory	Grants access to authorized resources
ExpiresIn	Number	Mandatory	Token expires in 3600s
TokenType	String	Mandatory	Bearer
IdToken	String	Mandatory	Used in the Authorization Header that identifies a user

4.3 Change Password API

The Change Password API allows an authenticated user to change their existing password to a new password.

Reference URL: https://tvs-cbp.com/api/auth/changePassword **HTTP Method:** POST		
Message Direction	**Format**	**Body Example**

Request	JSON	{
		"OldPassword": "OLD PASSWORD",
		"NewPassword": "NEW PASSWORD",
		"AccessToken": "ACCESS TOKEN"
		}

Response	JSON	{
		"Result": "Success"
		}

4.3.1 Change Password Request Message Elements

Data Element Name	Format	Disposition	Comment
OldPassword	Old password	Mandatory	Request to enter old password
NewPassword	New password	Mandatory	CBP Password Policy: • Minimum Length: 12 • Requires at least 1 Number • Requires at least 1 Special Character • Requires at least 1 Uppercase Character • Requires at least 1 Lowercase Character
AccessToken	Access token	Mandatory	

4.3.2 Change Password Response Message Elements

Data Element Name	Format	Disposition	Comment
Result	String	Mandatory	Returns “Success” or errorMessage

4.4 Authentication Service Errors

The following errors may be observed when calling the Authentication Service. CBP recommends that the camera device provide feedback to the camera device operator when errors occur. This greater level of detail will facilitate the communication of errors for troubleshooting.

Message	Definition	Recommended Display
Authentication failed	Username or Password provided is incorrect	Username and/or Password provided is invalid, please provide a valid Username and/or Password
Invalid Input	Incorrect input fields	Input fields are missing or invalid, please enter all the required and valid input fields
Password did not conform with policy: Password must have lowercase characters	Password does not contain at least one lowercase character	Password must contain at least one lowercase character
Password did not conform with policy: Password must have numeric characters	Password does not contain at least one numeric character	Password must contain at least one numeric character
Password did not conform with policy: Password must have symbol characters	Password does not contain at least one symbol character	Password must contain at least one symbol character
Password did not conform with policy: Password must have uppercase characters	Password does not contain at least one uppercase character	Password must contain at least one uppercase character
Password did not conform with policy: Password not long enough	Password does not meet the minimum length	Password length must be at least 12 characters
Attempt limit exceeded, please try after some time.	User exceeded the number of allowed failed attempts.	Password reset limit exceeded, please try again after sometime.

5. TVS Environments

5.1 TVS in a Box

"TVS in a Box" (TIAB) is a virtual instance of TVS that simulates the environment and services to allow developers to code and test in a sandbox environment. This environment is to be used during the Development Step of the Project Plan Process. When ready to access TIAB, please contact CBP for user credentials.

5.2 SAT Environment

The SAT environment is TVS's test environment for technical certification. This environment is for use during the Testing Step of the Project Plan Process. The following URL is to be used for the SAT environment: https://sat.tvs-cbp.com. The TVS SAT environment is subject to ongoing development and may undergo periods when it is unavailable. When ready to access TVS SAT, please contact CBP for user credentials.

5.3 Production Environment

Upon successful technical certification, access to the TVS production environment will be provided. The production environment is the live instance of TVS. This environment is to be used during the Deployment Step of the Project Plan Process. Prior to deployment, but after TIAB and

TVS SAT testing, the production URL and user credentials will be provided by CBP.

6. Contact Information

Send questions and comments related to this reference guide to tvssupport@cbp.dhs.gov.

Include in the email:

- Stakeholder CBP POC
- Stakeholder Name
- Port Name
- Description of the Issue
- POC with Email