Implementation Guide

Overview

The SheerID Implementation Guide provides an overview of topics, features and resources of interest to integrators and implementers of SheerID eligibility verification services. Content is designed for business and technical stakeholders. Links to more detailed online documentation and white paper resources are incorporated here and should be consulted by technical stakeholders for complete details.

Contents

Implementation Guide

Accounts – Sandbox and Production

An account is required to initiate a SheerID implementation. User accounts for the SheerID sandbox environment are created from the [account signup page](#).

The sandbox environment is used for development and QA purposes. In this environment, verification results can be simulated to enable complete instant and document review use-case testing, using only fictitious data[1].

With a user account, you can [login to the sandbox SheerID Control Center](#) portal to utilize a collection of implementation related tools and post-implementation services.

The sandbox and production environments utilize separate repositories for user account, passwords, access tokens, templates, notifiers, and other configuration artifacts. Changes to sandbox environment components will not directly affect the corresponding production component.

User accounts are promoted from the sandbox environment to the live production environment by SheerID staff. Production account activation requires an executed Master Services Agreement and follows confirmation that the sandbox implementation demonstrates all expected behavior required for production use. When an account is promoted, users can [login to the production Control Center](#) portal.

---

[1] See [Sandbox Verification Source](#) and [Sandbox Automate Document Review](#)

Verification Types and Field Requirements

Verification Types

Several types of verification are supported. Implementations should include Asset Review verification whenever applicable, to insure that 100% of eligible audience has a verification opportunity.

- **AUTHORATATIVE** – verification is conducted against one or more data sources providing confirmation that the field data submitted matches an authoritative data source
- **ASSET_REVIEW** – verification is conducted by document review specialists to confirm the document uploaded is a valid document type, and includes data required for verification
- **VALIDATION –** verification is based on a match of submitted organization ID and email address domain against a configured set of valid domains for that organization ID
- **EMAIL_LOOP –** can be used in conjunction with VALIDATION or by itself, verification is based on successful receipt and click-through of a tokenized link delivered to a specified email address
- **IP_ADDRESS –** verification is based detection whether the IP address that verification subject is coming from is associated with a specific (UNIVERSITY) organization ID
- **SSO** – available for compatible UNIVERSITY organizations only, verification is based on a successful login to the school portal using school-provided user credentials
- **HONOR_SYSTEM** – verification is always returned as successful when data field requirements are met

Affiliation Types

Verification sources are consulted based on the Organization and Affiliation Type specified in a verification request.

Organization Type	Affiliations
Military	Active Duty Veteran Reservist Military Retiree Military Family Disabled Veteran Civilian Employee
University	Student_Full_Time Student_Part_Time Graduate - separate from enrollment verification service Alumnus - separate from enrollment verification service Faculty
K12	Faculty
First Responder	Police Firefighter EMT
Membership	Member
Corporate	Employee
Custom Data Sets	*Custom Data Sets*

Data Field Requirements

Data Field Requirements vary by Verification type and Affiliation type. Please review the (minimum) data requirements for any organization, affiliation and verification types.

Extra fields can also be collected, stored as request metadata, and are available for reporting purposes. Hosted implementations can populate extra fields from dynamic URL parameter input such as UTM codes, and pass back this data or report it on demand.

Eligibility Verification User Flow

Refer to this document for a diagram of the general flow of a SheerID Eligibility Verification user experience for hosted or API implemented applications.

SheerID customers are encouraged to incorporate both instant verification and (asynchronous) secondary document review verification capabilities into an eligibility verification application. This ensures that 100% of eligible participants have an opportunity for eligibility verification.

General API Developer Guidelines

Several important API Integration topics, including:

- API Authentication
- Issuing Requests
- Request Rate Limiting
- API Date Formats
- API Error Codes and Conditions

are discussed in more detail under General Developer Guidelines and Issuing Requests.

REST API Resources for Basic Verification Applications

A small subset of the available REST API endpoints are required to construct a complete verification application. The primary services most frequently used to implement a basic API-driven verification workflow include:

Required Fields

- List Fields - Obtain a map of required fields for the specified Verification Types

Verification

- Verify - Perform a verification. This is the primary method of importance for most integrations
- Inquire – Check the status of a historical verification request
- Update Verification – Update and re-submit an existing verification request

Asset

- Issue Token – Issue a token to facilitate Document Review via Asset Upload
- Upload – Upload an asset for review

A complete listing of SheerID REST API endpoints is available online.

A number of sample API code recipes are also available online on the SheerID GitHub Getting Started / Recipes page.

Notification

Notification services include customer-oriented Verification Email messaging, and server-to-server event notification, providing complete flexibility in designing a verification user experience.

Customer oriented Verification emails

Customer oriented Verification emails are HTML brand-able, with fully customized content for success and consolation messaging. Verification emails are utilized in SheerID-hosted implementations and are optionally available for use in API integrations.

HTTP Notification

HTTP (server-to-server) Notification can be configured for more specialized or customized user experience requirements. This event handler sends an HTTP request (a "webhook") to a specified callback URL on your site for each change in state for verification requests submitted on your account or web template. Your callback URL will include **requestId** as a parameter. The notifier may be configured to use either GET or POST method. With the POST method, you have the option to receive additional data in form post or JSON format.

Notification Filters

By default, notification fires for all **requestId** state changes. It is possible for one verification request to generate several notifications as it moves through its lifecycle.

A filter can be configured to limit notifications to specific statuses only. A common filter use case is document review notification for ASYNCHRONOUS_UPDATE events - once a decision has been rendered for an uploaded document. Notifier filters must be applied by SheerID staff. We are happy to consult with you and to assist with any Notifier configuration or filter configuration assistance you require.

Same Person Limits

SheerID verification can be configured to track and limit the number of times the same credentials are successfully used for verification. This is a useful feature when offer access limiting is important.

The same person limit feature can be used to set a policy on the number of verifications allowed for a particular individual over a period of time. It can be configured as part of a hosted implementation, or can be supplied by the API integrator as request configuration. Your policy can specify the data definition and expiration period for any limits. When an end-user has exceeded the number of allowable verifications by policy, the API will refuse to process the verification request and instead return an error code. A hosted implementation will present a customizable error message. By default, no same person limits are defined.

Reward Management / Reward Mapping

Reward Pools provide SheerID customers' the ability to import a list of pre-determined codes to be issued as primary or consolation rewards following eligibility verification. The types of data most frequently used in reward pools include single-use coupon codes, unique access codes, and product activation numbers. Static rewards, such as a static Promo Code, can also be configured within hosted implementations and periodically updated.

Reward data can be recorded as extra field metadata and included in verification reports or **requestId** Inquiries, allowing for flexible tracking and intelligent follow-up messaging to promote reward conversion.

Reward pools are configured with a threshold value to trigger email notification to you when reward inventories reach a specified threshold. Reward pool inventories can be viewed or updated through the production Control Center.

Complex verification reward mapping and conditional reward behavior can be configured through the Reward Management utility. SheerID staff can consult and assist when applications for this capability are required.

JSAPI Utilities

SheerID's JavaScript API provides functionality that can be integrated into user-facing web applications. Utilities include:
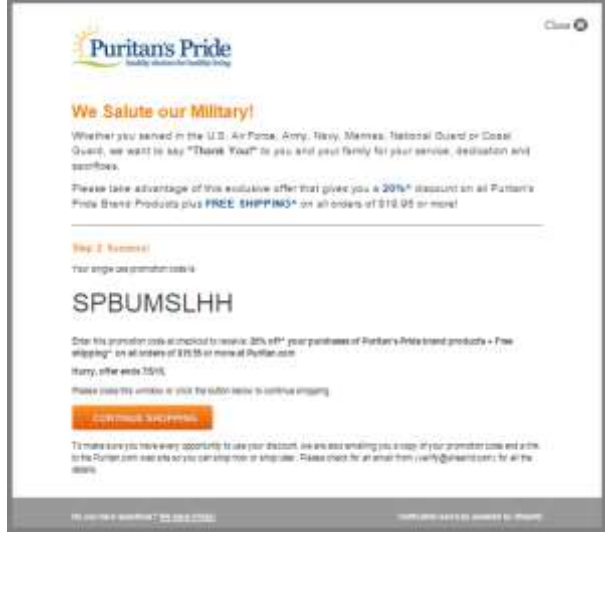
- Organization Combobox – simplify organization selection with a type-ahead select list
- Iframe deployment – simplify setup of a responsive, SheerID-hosted iframe
- Token redemption – a client-side method for redemption Token processing
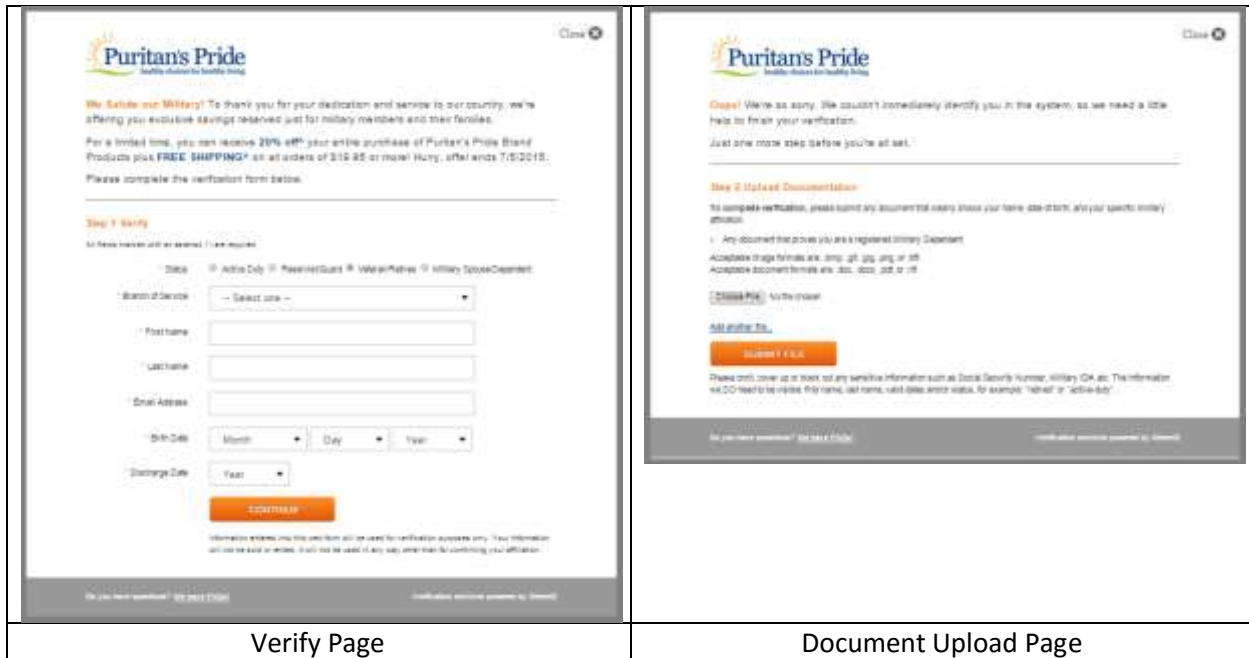
Hosted Implementations

SheerID hosted implementations provide a custom branded verification user experience that can be easily integrated with you own online properties. Hosted implementations are delivered through full landing / interstitial web pages, or through iframes that pop-up (light box) or are embedded within your own web page(s).

Typical User Experience

A typical eligibility verification user experience requires only 2 steps – information is collected for verification and a success page is presented with reward and call to action instruction. When an instant verification can't be made, a document upload page is presented and verification results and reward / conversion instructions are delivered by email.

| Verify Page | Success Page |

Verify Page	Document Upload Page

Pre-populating hosted Verification forms

Hosted implementation form fields can be pre-populated when that information is available. Both GET and POST HTTP request methods are supported. Review details here.

Redemption Token integration

SheerID redemption tokens provide a robust offer protection mechanism for a hosted implementation, when other mechanisms such as single-use coupon codes are not available. Redemption tokens are unique, single use values passed back on a personalized success URL. REST API resources allow you to check the validity of a token, and redeem or revoke the token when that is appropriate to your objectives.

RequestId integration

For more specialized integration with a SheerID hosted implementation, the **requestId** can be passed back as a parameter on a personalized URL. Using the Inquire and/or Get Person API resources, integrators can review verification status and extract field data collected by the hosted implementation for use within custom business logic.

Control Center

Overview

The SheerID Control Center portal is a collection tools and services to support implementation and post-live customer needs. Both Sandbox environment and Production environment Control Center portals are available. All content for each environment is maintained separately, so that changes to one environment will not automatically be applied to the other.

The sandbox control center login page is: https://services-sandbox.sheerid.com

The production control center login page is: https://services.sheerid.com

Passwords

Password Reset - Control Center passwords can be reset at any time by using the "Forgot your password?" link on the Control Center login page. Enter your username on the Password Reset Request page and password reset instructions will be sent to the email address on file for this username.

Password Complexity –Passwords must be at least 8 characters in length, and must be comprised of at least one character from each character class: upper-case, lower-case, number, and symbol.

Password Expiration – Passwords will expire after 90 days. When attempting to login after a password has expired, an email will be automatically generated to the email address on file for the affected username, containing a link to reset your password. Your previous 5 passwords cannot be reused when resetting your password.

Password Lockout – Accounts are locked after 5 (consecutive) unsuccessful login tries within a 12 hour period. Locked accounts can be unlocked by using the Password Reset link to have password reset instructions emailed to the email address on file for this username.

Manage Users and Roles

Once an account is created, additional users can be added and their roles managed by the account holder or any other user with the User Admin role. Providing all users with individual login credentials is recommended.

API Access Tokens

One or more API Access Tokens can be issued to facilitate access to protected REST API resources. Users have complete control over API Access Token lifecycles. SheerID Secret Tokens can also be revoked and regenerated, and used to verify the signature of notifications and hosted verification redirect URLs.

Configure Notifier

Use this tool to configure a callback endpoint for HTTP notification. Select from GET or POST method, optionally rename the parameter for **requestId**, and select the data format for POST method notifications.

Web Templates

Web templates are used to configure SheerID hosted implementations and can optionally be used by API integrators for simplified, persistent request configuration. When used to configure API request parameters, the **templateId** is included within a verification request. This sample API code recipe demonstrates this usage.

Verification Email Management

HTML-branded email messaging can be configured for instant and document review verification result notification. Different messaging is configured for success and consolation results.

Verification Reports

Verification reports provide on-demand extracts of verification activity, for any time period, in a csv format. Reports can include standard field content and custom, extra field metadata.

Verification Consoles

Verification consoles provide an interface for submitting instant and document review verification requests on behalf of the verification subject, for selected affiliation types.

Customer Service Search

The Customer Service Search tool allows you to look up the status of historical requests by name or email address, and review more information on a verification request including customer details, configured metadata, document review details, emails sent, HTTP notifications, and a document upload option for non-completed / non-expired requests.

Reward Management

The Reward Management tool allows you to create, view, or update rewards and reward pools used with hosted or API implementations. Notification can be triggered when reward inventories reach a specific threshold.

API Project Planning and Implementation Checklist

Design Phase	Create Account		
		☐	Create Sandbox Account
		☐	Add / Manage Users
		☐	Issue Sandbox API Access Token
	Review Documentation		
		☐	Review REST API Documentation and other resources to determine implementation path for your needs
		☐	Review best practice recommendations
		☐	Review verification field requirements
		☐	Review template request configuration options
		☐	Review Getting Started Sample Recipe Code
	Technical Kick-off		
		☐	Schedule kick-off meeting with the SheerID technical team to review project scope, discuss technical questions, and coordinate assistance required
		☐	Set up periodic implementation status / consulting reviews with SheerID team
Implementation Phase	Create Verification Service		
		☐	Design/Implement Presentation Layer - Organization Combo box for School/ID selection
		☐	Configure Template Verify Request Configuration
		☐	Determine / Implement Strategy for Asset Upload - Client implemented - SheerID hosted, define branding requirements, upload instructions
		☐	Configure HTTP Notifier, Filter if applicable
		☐	Configure Verification Email Messaging if applicable
		☐	Configure Same Person Limits if applicable
		☐	Configure Primary, Consolation Reward if applicable
	User Acceptance Testing		
		☐	Review Sandbox Verification Source and Automate Document Review Instructions to test all instant and document review use-cases
Final Pre-live check and launch	Readiness Review		
		☐	Demonstrate final implementation with SheerID staff for readiness confirmation and post live support preparations.
		☐	Determine any special Document Upload or Document Review criteria
	Activate Live Implementation		
		☐	Activate Production Account
		☐	Migrate or configure templates and notifiers from sandbox environment
		☐	Delegate Asset Review to SheerID Document Review Specialist team
		☐	Production Smoke test / Soft Launch to re-confirm live functionality
Post Live Support	Post Live Operational Tools and Support		
		☐	Introduce SheerID contacts for Client Services and verification Customer Service
		☐	Provide orientation to Control Center tools, including Verification Reporting Options and other relevant tools
		☐	Coordinate any marketing or promotional campaign assistance with SheerID team