BRIDGE

Bridge Protocol Network MVP Overview

Contents

System Capabilities and Service Model

This documentation serves as an overview for integration with Bridge Protocol's Identity Platform. The platform provides seamless enterprise adoption functionality such as:

1. Trusted clearinghouse - Secure handling and clearing of user data after verification
2. Verified ID assigned to NEO public address for portability and anonymity; for use throughout exchanges, businesses and ICOs

Identity Report

The *Identity Report* provides validation of an applicant's address, date of birth (DOB), name and mortality by cross referencing a range of verified databases. Additional options for United States compliance, include request for Social Security number through the full 9 or last 4 digits.

Document Report

The *Document Report* is composed of data integrity, visual authenticity and police record checks. The system checks most recent identification documents and checks for discrepancies. A human verification is required when the image is obscured, blurry or cropped.

Check Types

The Bridge Protocol has compliance capabilities for over **165 countries**, using standard and express checks.

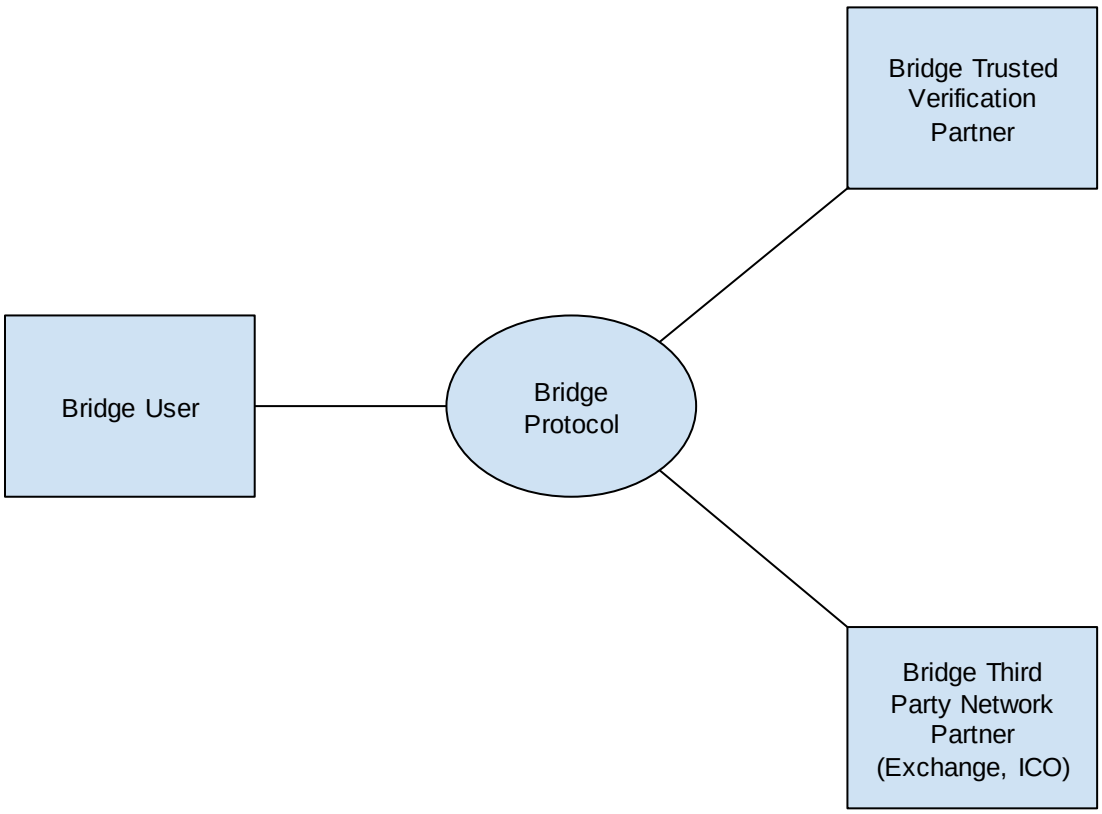
A **standard** check requires an applicant to enter their information via our applicant form.

An **express** check bypasses this process and requires all the applicant's information be provided by the client application.

Bridge Protocol Network

Bridge Protocol facilitates interaction between Bridge Users, Trusted Verification Partners and integrated Network Partners. This combination creates a robust, scalable and secure digital identity authentication platform.

By integrating with the Bridge Protocol Network, third party services satisfy their compliance requirements by establishing eligibility of the user; all while the user still maintains anonymity and total control of their personal data.



Bridge Passport

The Bridge Passport is the key to authentication, authorization, and data verification on the Bridge Protocol Network. Users can purchase a passport from Bridge Protocol with TOLL and provide their own key pair (Bring Your Own Key) to establish their own secure and personal digital identity on the platform.

This passport can be used to authenticate with third parties to provide anonymous access to their services, as well as allow third parties to determine the authorization level of the user via the Bridge Authorization Profiles associated to the passport. Bridge Passports also contain an associated NEO blockchain address to facilitate payment of fees in TOLL, allowing the user to take advantage of Initial Coin Offerings (ICO) that require NEO transactions and provide robust supplemental data verification functionality via the blockchain.

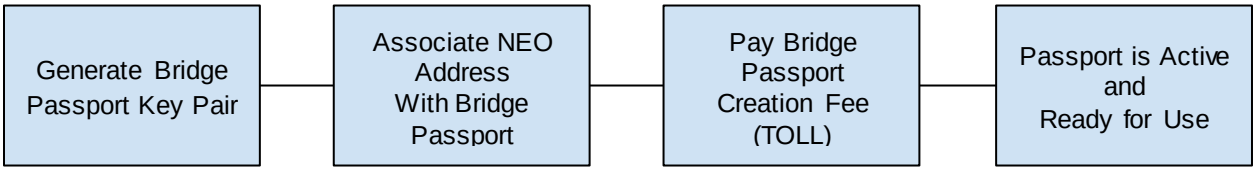
Bridge Passports can only be created via the Bridge platform, but the keys that establish digital identity are created and managed by the end user. The only control Bridge maintains over a passport is the right to revoke a passport if the address is deemed to be a bad actor and a risk to the security and integrity of the platform.

In the future, Bridge Protocol will offer functionality to allow users to use hardware based key storage devices to protect their Bridge Keys and use them on the platform. It is important to note that Bridge does not store or ever have access to the user's Bridge Keys, Associated NEO Address, or Bridge Authorization Profiles.

All keys and data are exclusively managed and stored by the user.

Bridge Passport Creation Process

The Bridge Passport creation process allows the user to bring their own keys and to associate a NEO address that they control. The process:



1. The user generates a key pair themselves or via the Bridge Client
2. The user associates a valid NEO Address with their Bridge Passport
3. The required amount of TOLL is paid to create the Bridge Passport
4. The Bridge Passport is created on the network and is available for use

Bridge Authorization Profile

Bridge Authorization Profiles are created for the user using the set of verified claims received from the Bridge Trusted Verification Process and stored as part of the user's Bridge Passport. These profiles can be furnished to third parties integrated with the Bridge Protocol Network to anonymously establish the user's authorization levels to the third-party platform and services.

Bridge Authorization Profiles each have a different purpose and scope, and also have a default expiration depending on type. Further flexibility is offered to third party authorization partners to define their own accepted expiration windows depending on their organizational compliance requirements.

Once created, the Bridge Authorization Profile has no personally identifiable data, and is encrypted so only the associated Bridge Passport can decrypt and view the data.

Bridge Authorization Profile Types

At current, the Bridge Authorization Profile types are focused around age verification and KYC compliance requirements.

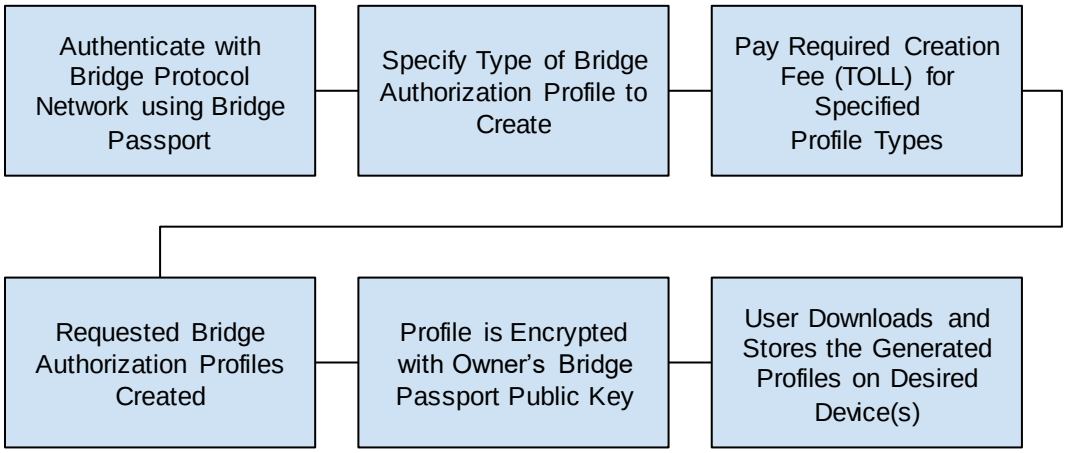
The current profiles offered by the Bridge Protocol Network MVP:

- Age Verification (18+)
- Age Verification (21+)
- KYC Level 1 (Age, DOB, Name, Email)
- KYC Level 2 (All Prior and document checking, watchlists)
- KYC Level 3 (All Prior and Accredited investor status)

Bridge Authorization Profile Creation Process

The Bridge Authorization Profile creation process takes place after a user has successfully completed Bridge Trusted Verification process and received their set of signed verified claims from the partner.

To create a Bridge Authorization Profile, the user:

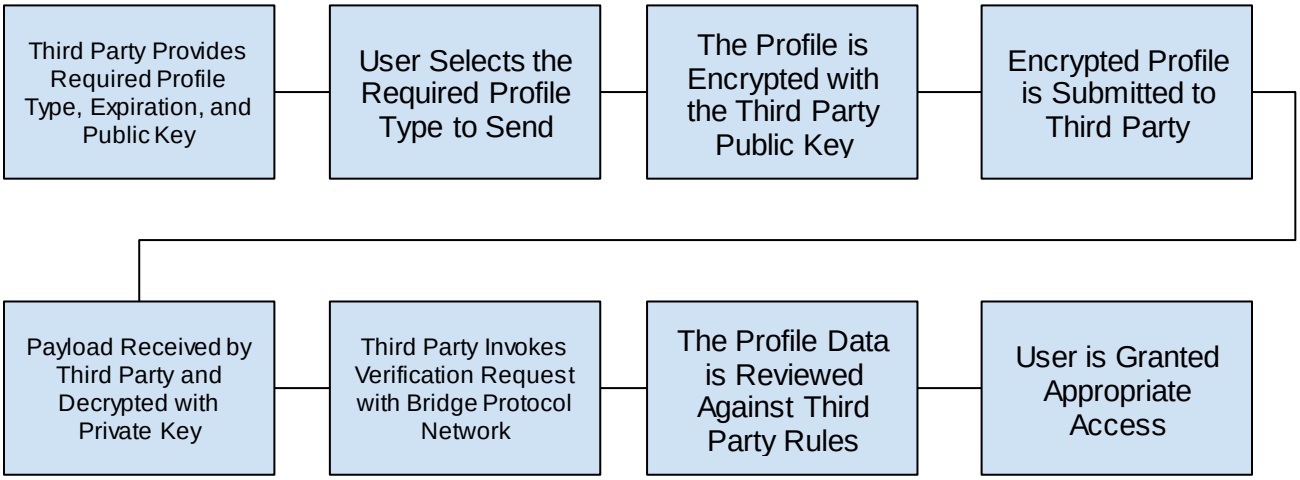


1. Provides their Bridge Passport to authenticate and gain access to Bridge Protocol Network services
2. Specifies the requested type of profiles they want to create
3. Provides the required TOLL to cover profile creation fees for the specified profile type(s)
4. The profiles payloads are generated for the user using the verified claims resulting from the Bridge Trusted Verification Process, and the hash is recorded with the Bridge Protocol Network
5. The profile payload(s) is/are encrypted for the end user using their public key
6. The user downloads their generated profile(s) and stores the file(s) on their desired device(s)

Bridge Authorization Profile Submission Process

Bridge Authorization Profiles are stored, managed and transported by the user directly to the integrated third-party platform or service. Bridge Protocol never has access to the data payload, the encryption keys, or has any involvement in the transport of a Bridge Authorization Profile from user to third party verifier.

To use a Bridge Authorization Profile to determine authorization with a network integrated third party service provider, the user:



1. The user visits the third-party site or service requiring Bridge Authorization Profile verification and receives the Bridge Passport public key of the third party
2. The user chooses the required Bridge Authorization Profile from their device that meets the requirements of the third-party service
3. The desired profile is encrypted with the third party public key for secure transport to the third party
4. The encrypted payload is submitted to the third party
5. The third party receives the payload and decrypts the payload with their Bridge Passport private key
6. The third party invokes a verification request on the Bridge Protocol network and pays the verification fee (TOLL) to verify the data integrity of the received Bridge Authorization Profile
7. The third party reviews the profile data (creation date, expiration, verified claims) and determines the eligibility of the profile based on their own criteria or compliance requirements
8. The user is granted the appropriate level of access / authorization

Bridge Trusted Verification Partners

Bridge Trusted Verification Partners are network partners that offer Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) claims verification services to the users on the network. The claims that are verified by these third parties enable users to create one or more Bridge Authorization Profiles. These profiles enable the user to interact with third parties that are integrated with the Bridge Authorization Platform to establish anonymous authorization to their services.

The premiere verification partner on the Bridge Protocol Network is Bridge KYC (provided by Bridge Corp, powered by Onfido). In the future, organizations will be able to integrate with the network as a Bridge Trusted Verification Partner and receive TOLL in exchange for the verification services they provide to the network.

Bridge KYC Verification Capabilities

The Bridge KYC currently supports all required verification checks to produce the set of verified claims that Bridge Protocol requires for the user to be able to create all of the Bridge Authorization Profile types available on the network today.

The Bridge KYC supports both express and standard check capabilities for over 165 countries that include (but are not limited to) the following verifications:

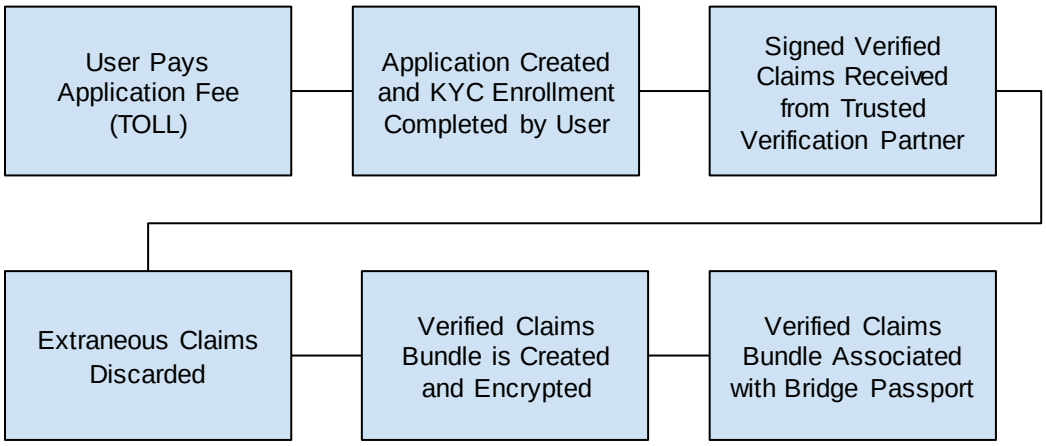
- * Identification Document Integrity
- * Visual Authenticity Applicant Address
- Date of Birth (DOB)
- Name and Mortality
- Social Security Number (SSN - US Only)
- Criminal History
- Street Address Verification

* In the event that there are discrepancies in identification documents or visual authentication issues with image quality, human verification may also be required to verify the requested claims.

Bridge KYC Verification Process

The Bridge KYC claims verification process allows the user to securely provide their personal data to our KYC provider (Onfido) and send Bridge Protocol the set of verified claims that will allow the user to create their desired Bridge Authorization Profiles on the network.

The claims verification process:



1. The user pays the required Application Fee in TOLL to the Bridge Protocol Network
2. * The application is created, then the user provides all the requested documents and data to satisfy the Onfido KYC enrollment process
3. Once the KYC verification is complete, the set of verified claims will be individually signed by the verification partner (to ensure integrity and prevent tampering), and securely sent back to Bridge Protocol
4. The verified claims are then scrubbed for any personally identifiable data and any claims not explicitly needed by Bridge Protocol to create Bridge Authorization Profiles will be discarded
5. Each relevant claim will be added to a payload that is signed and encrypted with the owner's public key
6. The bundle of verified claims is associated with the user's Bridge Passport and is available for future use in the creation of Bridge Authorization Profiles

* Details about the data retention and security policies for the user data submitted in the application process can be found here: https://onfido.com/gb/security/

Third Party Platform and Service Integration

Integration with the Bridge Protocol Network allows third parties such as Exchanges, ICOs, and websites to take advantage of robust authentication, authorization, and data verification services to ensure compliance. Bridge Protocol provides API documentation, SDK libraries, and sample projects to Bridge Network Partners to empower them quickly and seamlessly integrate Bridge Protocol Network functionality into their platform or service.

Bridge Authentication Platform

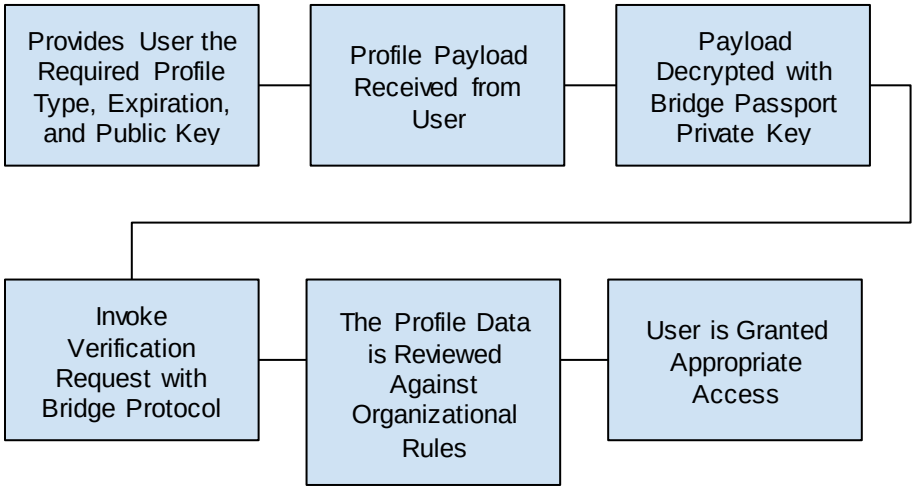
The Bridge Authentication Platform enables the user to authenticate with the Bridge Protocol Network using their Bridge Passport and interact with network services such as Bridge Trusted Verification and Bridge Authorization Profile creation services. In the future, the platform will be available to third parties to allow for Single Sign On (SSO) and anonymous authentication to their platforms and services.

Bridge Authorization Platform

The Bridge Authorization Platform allows third parties to determine eligibility and grant authorization to their platform or service while still maintaining data security and anonymity to the user requesting access.

Bridge Authorization Profile Verification Process

Once integrated with the Bridge Protocol Network, the process for a partner to evaluate authorization levels using a Bridge Authorization Profile:



1. Provide the end user with their Bridge Passport public key to allow for secure transport of the profile payload
2. Receive the payload from the user
3. Use their Bridge Passport private key to decrypt the payload
4. Send a data integrity verification request to the Bridge Protocol Network and pay the required TOLL to cover the required integrity verification fees
5. Once verified, evaluate the data against the organizational and compliance authorization rules, and establish eligibility
6. Grant the user the appropriate authorization / access