PAI PASS

Summary of the Project PAI Authentication Protocol

Background

The fundamental vision of Project PAI was that we should all own, manage, and ultimately be able to harness the value of our own personal data. As a proof of concept to demonstrate how applications might be launched in such an ecosystem, Project PAI partnered with Oben to launch PAIYo, an application that enables users to harness their personal data to create personalized avatars. Oben successfully launched the PAIYo mobile app and the community response has made it clear that users are interested in a wider variety of ways to derive value from their personal data.The ability to create avatars in PAIYo served as a great proof of concept to validate the vision of Project PAI. However, Project PAI is about much more than personalized avatars.

To take the next step in building an ecosystem that enables users to own, manage, and ultimately harness the value of their own personal data, Project PAI is pleased to announce PAI Pass. PAI Pass was jointly developed by P19 Inc. and J1149 Inc, third party supporters of Project PAI. At its heart, PAI Pass Is a Single Sign-on (SSO) service that leverages Project PAI's data storage layer.

PAI Pass is designed to allow users to harness the full value of their data by opening up the features that allowed Oben to develop personalized avatars to other developers to offer users products and services that leverage their personal data. Project PAI, P19 Inc. and J1149 Inc. are pleased to announce that the PAI Pass codebase will be open source.

PAI Pass

PAI Pass is a new kind of Single Sign-on (SSO) service. Like existing SSO's, PAI Pass makes it easier for users to login to supporting applications ("Partner Applications"). In addition, PAI Pass allows users to populate their PAI Pass profile with new data created through their interactions with Partner Applications.

PAI Pass user data is encrypted via Elliptic-curve Cryptography and the users retain control of data associated with their PAI Pass profile at all times. PAI Pass users, and only users, have the power to decide whether, and how much, of their PAI Pass profile data to share with third parties.

Account Creation

PAI Pass accounts can be created directly through the PAI Pass web application. In addition, users can create PAI Pass accounts through Partner Applications that have integrated PAI Pass. In either case, the creation of a user account prompts the user to input certain information (e.g., email address and phone number).

Authentication Levels

Users that create accounts have the option to verify their accounts as well as certain attributes associated with their PAI Pass profiles. The status and level of verification creates the following classes of PAI Pass accounts.

Level 0 Accounts

A Level 0 User has created an account but has not verified that they control the email address or phone number associated with their profile.

Level 1 Accounts

A Level 1 User has created an account and has verified that they control the email address associated with their profile. However, a Level 1 User has not verified that they control the phone number provided by the user.

Level 2 Accounts

A Level 2 User has created an account and has verified that they control the email address and phone number associated with their profile.

Level 3 Accounts

A Level 3 user has created an account and has verified the email and phone number associated with their profile. In addition, Level 3 users have successfully completed the PAI Pass Video Authentication to verify their legal name.

Custom Status Accounts

In the future, Level 3 users may have the ability to become a “custom status” user. A custom status user is a Level 3 user who has gone through the Custom Status Verification process (as described below) to verify a custom attribute (*e.g.*, a professional credential or license).

Authentication and Verification Processes

PAI Pass enables users to authenticate and verify their data. Currently, users can only verify their email address, phone number, and legal name. However, the existing PAI Pass authentication and verification procedures could be used to support the verification of additional user data such as date of birth, citizenship, and address. In addition, the development of Custom Status Verification protocols could support a wide range of “custom status” accounts.

Users can recover their account via the ‘forgot password’ functionality. The sign-in flow includes a link to a forgotten password form, which allows the user to reset the password for their account. The main user email address and phone number can be changed in the user profile section of the PAI Pass web application after verifying the user’s password.

While there are no perfect identity and authentication systems in existence, PAI Pass is designed to be significantly more secure than other SSOs.

Email Address Authentication

To verify an email address, a PAI Pass user simply clicks a link included in an email message sent to the email address associated with their PAI Pass profile.

Phone Number Authentication

To verify a phone number, a PAI Pass user inputs the code sent via SMS to the phone number associated with their PAI Pass profile.

PAI Pass Video Authentication

The PAI Pass Video Authentication process requires a user to record a video where they speak the words or phrases displayed through the PAI Pass interface while presenting an official identification credential (e.g., drivers license or passport).

Custom Status Verification

The PAI Pass Video Authentication process will require a user to record a video where they speak the words or phrases displayed through the PAI Pass interface while presenting the required credential (e.g., notary license) which credential can be verified through a third party data source (e.g., state notary registry).

Data Sharing

Users must affirmatively grant third parties access to their PAI Pass data by accepting offers presented to the user through the PAI Pass dashboard or when using the PAI Pass SSO. Once users grant permissions to access their PAI Pass data, users can withdraw such permissions in PAI Pass. Note, however, that due to the nature of data, revoking permissions to access data will not necessarily prevent a party that has already accessed data from sharing data. It will, however, be clear that the user has not authorized further use or dissemination of the user's data.

In the future, users of PAI Pass will be able to share their information with other PAI Pass users by identifying a specific PAI Pass user or users and selecting specific data to be shared with such user(s)], or by participating in the PAI Pass Offer Network as described below.

PAI Pass Single Sign-On (SSO)

Developers of PAI Pass Partner Applications, and other third party developers, may also allow users to access applications using their PAI Pass. A user attempting to sign on to a new application or service using PAI Pass will receive a notification in PAI Pass that a developer has requested certain information. The notification will include the name of the requesting developer and the requesting application or service, along with the specific information requested. PAI Pass users must affirmatively approve the request before the developer will have access to the information.

Data Storage Layer

PAI Pass will utilize the Project PAI Data Specification ("PDP-2) for redundant information storage to broadcast certain encrypted data with the desired recipient's public key. Permissioning (or subsequent revocation) of the uploaded files for use by the intended recipient is achieved by a transaction, whose OP_RETURN field includes a URL pointer to the resource. The data can then be downloaded and decrypted with the recipient's private key.

PAI Pass Use Cases and Roadmap

PAI Pass is, at its core, a SSO. Like other SSOs PAI Pass enables users to use a single account creation process for all participating applications while reducing the administrative burden for developers. However, unlike existing SSOs, PAI Pass was designed and built to enable users to own, manage, and ultimately harness the value of their own personal data.

As such, while it is anticipated that PAI Pass initial use cases will be similar to those of existing SSOs, the unique design should enable the creation of applications and functionality that allow users to capture more value in exchange for sharing their personal data with developers.

Partner applications can integrate PAI Pass as an SSO in a similar way as other social sign-ins (Facebook, Google, Twitter, etc.). Developers can access the PAI Pass API, documentation, and examples to begin adding PAI Pass functionality to their application.

<u>Existing Project PAI Ecosystem Applications</u>

Because the PAI ecosystem does not have a SSO service, currently all Project PAI ecosystem applications must independently maintain their own account system. By using a common account system like PAI Pass, all user data in Partner Applications can be consolidated into a single profile. This enables the user to view all of their data. The user can then decide what data they want to share with other developers.

A PAI Pass user that signs on to an application or service using PAI Pass will receive a notification in PAI Pass that the application developer has requested certain information. The notification will include the name of the requesting developer and the requesting application or service, along with the specific information requested. PAI Pass users must affirmatively approve the request before the developer will have access to the information.

<u>New Project PAI Ecosystem Applications</u>

Developers of new Project PAI Ecosystem Applications can attract new users by allowing users to access their application using the PAI Pass SSO. In the future, third party developers will be able to offer users access to their application through the developer dashboard. Those offer requests are displayed to users via the PAI Pass offer network, where users can filter and accept offers. Users will be able to filter offers by most recent, data-type, and various rewards (ex. free access to a game).

Roadmap

PAI Pass Offer Network

While not currently available, the PAI Pass Offer Network will allow PAI Pass users to affirmatively opt-in to receive offers from third parties that wish to access PAI Pass users' data. PAI Pass Offer Network users will select the information that can be shared with third parties for the purpose of making such an offer (*e.g.*, user status, etc.). Developers will be able to use the PAI Pass Offer Network functionality to offer value to the user in exchange for the developer's access to the user's personal information.

Before information is shared with a third party, the PAI Pass user will receive a notification in PAI Pass that a third party has requested access to certain information. The notification will include the name of the requesting third party, along with the specific information requested, and the other terms of the applicable offer (*e.g.*, access to online service, premium functionality within an application, monetary value, etc.) as well as the terms applicable to the requesting party's access and use of such information (e.g., privacy policy). PAI Pass users must affirmatively approve the request before the third party will have access to the information.

PAI Pass Videos

PAI Pass - Client App Demo: https://youtu.be/JSp6dXaGJsA
PAI Pass - User Dashboard Demo: https://youtu.be/gHy0NLjqnHE