Auth key login

The Auth key login feature of the Paybis API offers a straightforward and secure authentication solution tailored for non-custodial and web3 providers who prioritize privacy and usability.

> ⚙ Prerequisites
>
> - Integration Type: Client-to-server API integration.
> - Receive confirmation from your Paybis integration manager that the Auth key login feature has been enabled for your partner account before implementing this feature.
> - Signing requests is mandatory.
> - Implement logic for generating and storing auth keys on per user basis.

How it Works

Partners use an auth key (a unique string value such as a UUID or private key, generated and managed internally) for user identification and authentication within the Paybis On/Off Ramp. This key should be included in the `partnerUserId` field of each transaction request associated with a specific customer.

1. **Initial User Session:** During the first session within the widget, the customer is prompted to enter and verify their email via OTP (One-Time Password).
2. **Subsequent Sessions:** For subsequent sessions, the partner should provide the correct auth key (`partnerUserId`) and set the `passwordless` flag to true. Assuming the email associated with the provided auth key exists within the Paybis system, Paybis generates a one-time token. This token can then be utilized by the partner as an additional URL parameter, facilitating automatic user authentication within the widget.

Integration Flow Steps

1. **Auth Key Setup:** Generate and securely store an auth key (e.g., UUID, private key associated with the given customer).

2. Ensure that the user has an active session in your app.
3. Call the server-to-server API endpoint POST /Private Request) with the `passwordless` flag set to `true` and `partnerUserId` (both are required) parameters.
4. **New user (first session):** The user undergoes standard authentication by providing their email and verifying it through OTP. Paybis establishes the association between the provided auth key and the customer's email address during this initial session.

Existing user (repeated session): Paybis system generates and returns the server-to-server POST /Private Request) endpoint response containing `oneTimeToken` along with the `requestId`.

1. Pass the retrieved `oneTimeToken` as an extra SDK parameter upon widget initialization or in query parameters if you are using the Direct URL Integration.
2. If the supplied `oneTimeToken` is valid, the customer associated with the email address linked to this key is automatically logged in to the widget. Consequently, the email verification step is bypassed in the widget journey.

> ⚠ `oneTimeToken` expiration is 15 min.

Updated 8 months ago

← Control transaction fiat, crypto and amount

Set payment method for Google Pay, Apple Pay, and Credit Cards →