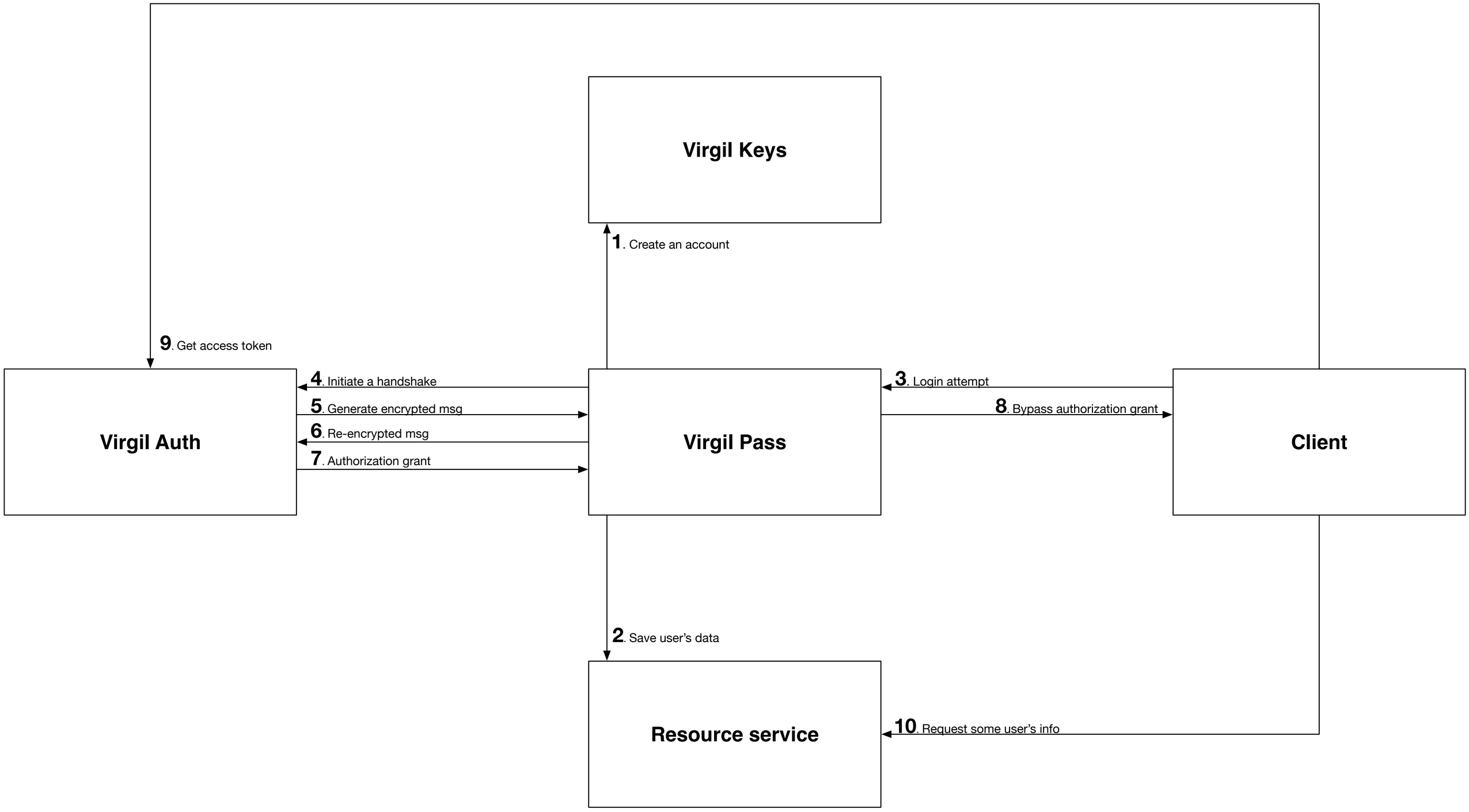

1. User creates creates a global *Virgil Card* on a **Virgil Keys** service that is supposed to be used by a **Virgil Pass** application for password-less authentication. It's possible to import a key pair for an existing *Virgil Card* as well.

2. Virgil Pass' User provides some information that will be shared with all the clients who'll use **Virgil Pass** for an authentication. This information gets saved on a **Resource Service**.

3. A **Client** application performs a login attempt. This action is intercepted with a **Virgil Pass** application that validates that an application is registered on a **Virgil Keys** service. The **Client** provides an application's *Virgil Card* uuid as a parameter.

4. **Virgil Pass** initiates a handshake with a **Virgil Auth** service providing one of registered global *Virgil Cards* uuids as a parameter.

5. **Virgil Auth** generates an encrypted message for a recipient as a handshake first step. This message contains a random message encrypted with User's public key.

6. **Virgil Pass** responds with a re-encrypted message.

7. **Virgil Auth** responds with an *Authorization Grant* code.

8. **Virgil Auth** bypasses an *Authorization Grant* code to a client.

9. **Client** exchanges an *Authorization Grant* for an *Access Token*.

10. **Client** uses an *Access Token* for requesting user's data on a **Resource Service**.