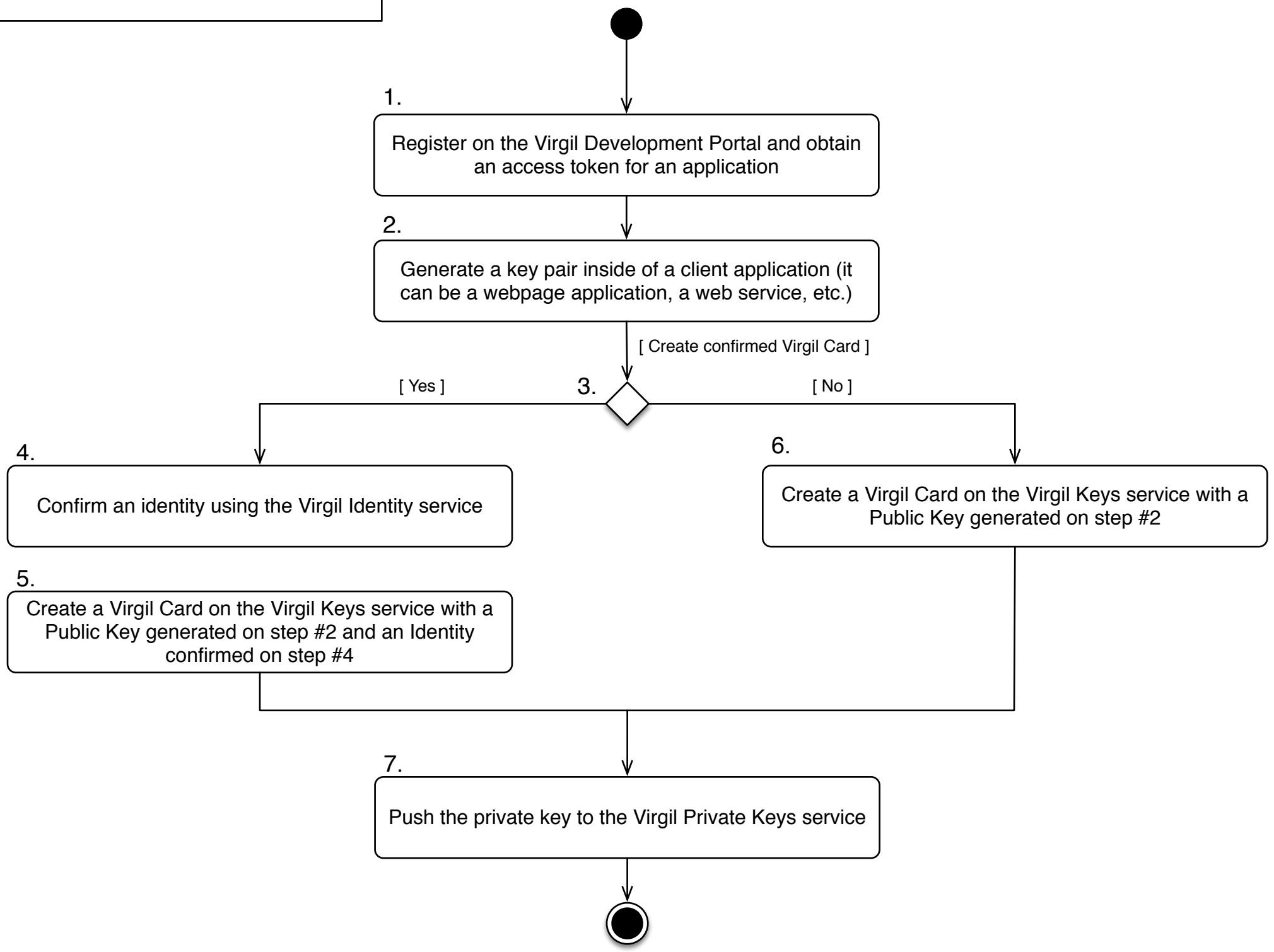
3.1. Create Virgil Card activity diagram



Legend

1. In order to perform calls to Virgil services it's necessary to retrieve the access token on Virgil Developers Portal (http://virgilsecurity.com).
2. Generate a key pair for a client application using appropriate VirgilSDK package. The key pair gets generated on a client to provide the full control for a user
3. There are two options to create a Virgil Card on the Virgil Keys service: create confirmed Virgil Card and create unconfirmed one. Confirmed Virgil Card grants that a holder of the Virgil Card owns the Identity (like email, mobile, etc.) and can be unambiguously identified. The unconfirmed on the other hand is almost anonymous user who can pretend that he controls the Identity he specified.
4. Confirm the identity on the Virgil Identity service. To make this, it's necessary to obtain the validation token by sequential invocation of /verify and /confirm endpoints of the Identity service.
5. To publish a public key and make a current user available for other users in order to exchange with per-to-peer encrypted messages, it's necessary to create a Virgil Card that combines an information about a Public Key and users's identity (like email, mobile, etc.). In order to create a confirmed Virgil Card (the card that definitely belong to a user) identity's validation token retrieved on the previous step is required
6. Create an unconfirmed Virgil Card by passing the Public Key value and Identity value.