New Signup using Facebook

To signup in any site we get more options like we can login with mail id, phone number, Google, face book, Amazon and so on. In that I worked on Face book Login.

The Facebook SDK for Android enables people to sign into our app with Face book Login. When people log into our app with Face book they can grant permissions to our app so we can retrieve information or perform actions on Face book on their behalf.

To do it we need to know about some important access controls provided as below.

* Go to Face book developer Portal

We need to go to the Face book developer site i.e. <https://developers.facebook.com/>. Here we get the information for the steps that we need to follow to create SDK.

To create any SDK we need access the tokens from the site those are as follows:

An access token is an opaque string that identifies a user, app, or Page and can be used by the app to make graph API calls. When someone connects with an app using Face book Login and approves the request for permissions, the app obtains an access token that provides temporary, secure access to Face book APIs. Access tokens are obtained via a number of methods.

The token includes information about when the token will expire and which app generated the token. Because of privacy checks, the majority of API calls on Face book need to include an access token. There are different types of access tokens to support different use cases:

* [User Access Token](https://developers.facebook.com/docs/facebook-login/access-tokens#usertokens): This kind of access token is needed any time the app calls an API to read, modify or write a specific person's Facebook data on their behalf. User access tokens are generally obtained via a login dialog and require a person to permit your app to obtain one.
* [App Access Token](https://developers.facebook.com/docs/facebook-login/access-tokens#apptokens): This kind of access token is needed to modify and read app settings. It can also be used to publish Open Graph actions. It is generated using a pre-agreed secret between the app and Face book and is then used during calls that change app-wide settings. You obtain an app access token via a server-to-server call.
* [Page Access Token](https://developers.facebook.com/docs/facebook-login/access-tokens#pagetokens): This kind of access token is similar to user access tokens, except that they provide permission to APIs that read, write or modify the data belonging to a Facebook Page. To obtain a page access token you need to start by obtaining a user access token and asking for the Page permission or permissions you need. Once you have the user access token you then get the page access token via the Graph API.
* [Client Token](https://developers.facebook.com/docs/facebook-login/access-tokens#clienttokens): The client token is an identifier that you can embed into native mobile binaries or desktop apps to identify your app. The client token isn't meant to be a secret identifier because it's embedded in apps. The client token is used to access app-level APIs, but only a very limited subset. The client token is found in your app's dashboard. Since the client token is used rarely, we won't talk about it in this document. Instead it's covered in any API documentation that uses the client token.

In these we are discussing about user access token and App access token in detail.

* User Access Token

Although each platform generates access tokens through different APIs, all platforms follow the basic strategy to get a user token:

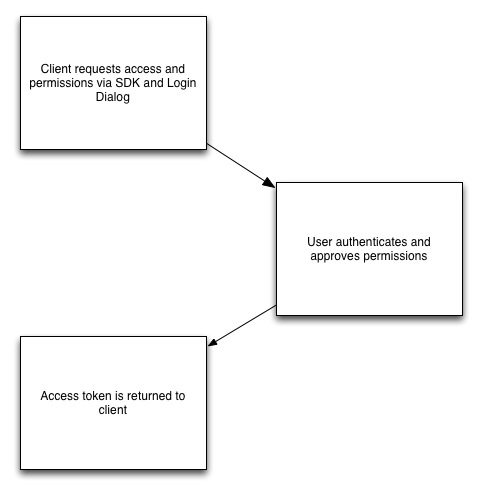


Fig 1: User Access Token

User access tokens come in two forms: short-lived tokens and long-lived tokens. Short-lived tokens usually have a lifetime of about an hour or two, while long-lived tokens usually have a lifetime of about 60 days.

One important aspect to understand about access tokens is that they are portable. Once we have an access token we can use it to make calls from a mobile client, a web browser, or from your server to Face Book's servers. If a token is obtained on a client, we can ship that token down to our server and use it in server-to-server calls. If a token is obtained via a server call, we can also ship that token up to a client and then make the calls from the client.

Different platforms have different methods to kick off this process.

* App access Tokens

App access tokens are used to make requests to Face book APIs on behalf of an app rather than a user. This can be used to modify the parameters of our app, create and manage test users, or read our app's insights.

Some user data that would normally be visible to an app making a request with a user access token isn't always visible with an app access token. If we're reading user data and using it in our app, we should use a user access token instead of an app access token.

Generating an App access token – To generate an app access token we need:

1. Our App ID

Before you can implement any of our products and SDKs or access any of our APIs, you must first register as a Face book developer and use our App Dashboard to provide information about your app. These documents explain how to register as a developer, how to use the App Dashboard to configure your app's settings, and how to build, test, and release your app. To do it we need to follow steps as below:

1. Register: Register as a Face book developer to gain access to Face book app development tools.
2. Create an App: Use the App Dashboard to create an app and access app and account settings.
3. Build and Test: Tools and information to help us with the app development process.
4. Release: How to make our app available to Face book users.
5. Maintaining Data Access: How to avoid losing access to Face book products, APIs, and SDKs.
6. Terms and Policies: Terms and Policies that we must agree to.
7. Support: Face book developer support resources and how to access them.
8. Our App Secret

The App Secret is used in some of the Login flows to generate access tokens and the Secret itself is intended to secure usage of our App to only those that are trusted. The secret can be used to easily create an App Access Token which can make API requests on behalf of any user of the app, which makes it extremely important that an App Secret is not compromised.

Therefore the App Secret or an App Access token should never be included in any code that could be accessed by anyone other than a developer of the app. This applies to all methods of code that are not secured like client-side code (such as HTML or JavaScript) or native apps (such as iOS, Android or Windows desktop apps) that could be decompiled.

We recommend that App Access Tokens should only be used directly from our app's servers in order to provide the best security. For native apps, Face Book suggest that the app communicates with our own server and the server then makes the API requests to Face book using the App Access Token. For this reason, if our 'App Type' under [Advanced Settings in the App Dashboard](https://developers.facebook.com/apps/) is set to Native/Desktop Face book assume that our native app contains the App Secret or an App Access Token in the binary, and Face book do not allow calls signed with an App Access Token to proceed. The API will behave as though no access token was provided.

If our App Secret is compromised, we should reset it immediately in the [Basic Settings of your App Dashboard](https://developers.facebook.com/apps/). When we start the reset process, we can specify a number of hours that the compromised secret will continue to work for when making requests, however anything sent from Face book (such as signed requests) will use the new secret straight away, so we must adjust our code to expect it as soon as possible.

* Permissions:

When a person logs into your app via Face book Login you can access a subset of that person's data stored on Face book. Permissions are how you ask someone if you can access that data. A person's privacy settings combined with what you ask for will determine what you can access.

Your app has requested a person's email address and the things they like but that request also automatically asks for access to a person's public profile. Your app can ask for additional permissions at any time, even after a person logs in for the first time. The additional permissions like ads\_management, ads\_read, business\_namangement, groups\_access\_member, Instagram\_basics, pages\_events, user\_birthday, user\_age\_range, user\_friends, user\_gender, user\_hometown, user\_likes, user\_link, user\_location, user\_photos, user\_paste, user\_vidios etc.

Face book Login allows **a person to grant only a subset of permissions** that we ask for to our app, except for public profile, which is always required. This is available as a separate screen in the login dialog when we ask for permissions. Our app should handle the case where someone had declined to grant our app one of the permissions we requested.

Once the development is over our app undergoes App Review. App Review is part of [app development](https://developers.facebook.com/docs/apps) that enables us to verify that our app uses Face Book Products and APIs in an approved manner. If our app will be used by anyone without a [Role on the app](https://developers.facebook.com/docs/apps#roles) or a [role in a Business](https://www.facebook.com/business/help/442345745885606?id=180505742745347) that has claimed the app, it must first undergo App Review. So that by doing this Face Book can manage the access of user details in the Face Book profile and restrict the unnecessary access, give permissions to only that app needs to function. It conforms that the app uses the data in intended ways and safeguards user privacy.