Connect your mobile app with OpenID Connect

If you have a native mobile app where users need to authenticate, you can improve security by adding federated authentication to your app. If you will implement federated authentication you should use OAuth as an identity layer. OAuth is directly related to OpenID Connect (OIDC) since OIDC is an authentication layer built on top of OAuth 2.0. Using this will allow your client to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in the form of claims. Read on to learn more about adding federated authentication in your app.

Best practices of apps and user authentication

How to setup your user authentication in apps is well documented. The Internet Engineering Task Force (IETF) has published a list of recommended best practices for security and user experience around use of these specifications in native apps. Read the Ping Identity blog if you want to know more about this. The Carnegy Mellon CERT also published a blog about good app authentication.

How adding federated authentication improves security

Offering your customers federated authentication the right way means end-users visually only hand off their password to their home organizations, and see their *familiar organization login page*. Opposed to this are app-developers offering their own in app login page: by doing that, users get more vulnerable to phishing attacks, since they get used to inputting their passwords in all kinds of apps. App-developers offering ‘the right’ way of federated authentication can use this in their sales pitch to new customers!

Ways of adding federated authentication in your app

You have a couple of options to do great authentication in your app:

- Ping Identity blogged about Google’s AppAuth they donated to the OpenID Foundation.
- GLUU also blogged about Google’s AppAuth initiative.

But my own in app login page looks far better!

One of the most heard objectives to ‘doing login right’ is that the user-flow or user-experience is worse than when you just offer input fields for a user id and a password. This might be true but the disadvantages don't outweigh that advantages. Please understand that companies like Google, Facebook and the Internet Engineering Task Force recommend 'their way' simply because this helps keeping the end user secure which is of the utmost importance.

Questions

If you want more information, please email us at support@surfconext.nl or return to our step by step guide.

Navigate