TECHNICAL INFORMATION

OpenID Connect

What is OpenID Connect?

OpenID Connect (http://openid.net/connect/) is an identity layer on top of the OAuth 2.0 authorization protocol (https://oauth.net/2/). OAuth 2.0 is described as "an open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications" (https://oauth.net/). While OAuth is a protocol for secure authorization, OpenID Connect makes identity a more integral part of the protocol and lets developers authenticate their users across websites and apps without having to manage passwords.

What are the benefits for end-users?

With OpenID Connect the end-users can securely access the services provided by a given merchant from desktop, web and mobile platforms (which we will refer to as user agents), as the protocol is widely supported. The protocol includes an approval step so the end-user can choose what information to share with the merchant he accesses, providing the end-user with a level of control few other protocols can match. Last but not least the user will not necessarily exchange password with the merchant as the protocol opens for delegation to well known secure identity providers (national and financial providers for example).

What are the benefits for merchants?

The wide support for devices and platforms of the OpenID Connect protocol also benefits the merchants as they can provide their business and reach end-users widely.

When used in its most secure mode (Authorization code flow) OpenID Connect does not trust the user agent used by the end-user. The Authorization code flow protects the end-user from various identity theft attacks. The information passed to the user agent does not include any information about the end-user, removing the responsibility of handling sensitive information at the user agent level. .

As the protocol is based on widely used technologies like JSON and HTTP and the fact that the protocol has been used for years, has made the protocol developer-friendly. The merchants will therefore be able to easily provide new secure services to its customers when using OpenID Connect.

OpenID Connect implementation

Authentication can be done in three different ways using OpenID Connect; the Authorization Code Flow, the Implicit Flow or the Hybrid Flow. Signicat currently supports the first and most secure one of the three; the Authorization Code Flow. The Authorization Code Flow returns an Authorization Code to the client. The client can exchange the code for an ID Token, an Access Token and optionally a Refresh Token directly with the OpenID Connect Authorization Server. This procedure provides the benefit of not exposing any tokens to the user agent (and possibly other malicious applications with access to the user agent).

Signicat also provides services protected by the OAuth Client Credentials (https://tools.ietf.org/html/rfc6749#section-1.3.4) allowing merchants to securely integrate with services in Signicat from their own systems.

SIGNICAT

Signicat is one of the leading providers of electronic identity and electronic signature solutions in Europe. The company, founded in 2007, delivers online trust based services to the public and private sector globally. The solutions are used by banks and financial institutions, insurance companies, government agencies and large corporations as well as small and medium sized businesses.

Signicat specializes in cross-border cloud based electronic identity services and electronic signatures. The company has local presence in Norway, Sweden, Denmark, Finland, the Netherlands and UK. These countries are in the forefront in the world with the usage of digital identities and electronic signatures.