Digi-ID app / website introduction

Digi-ID is an authentication method based on the security of the DigiByte blockchain. This allows you to log in to a website, application, building security and more by simply scanning or tapping on a QR code.

Digi-ID does away with the need for usernames and password, or it can be used to compliment them for additional security.

What's involved in integrating Digi-ID into my website / application?

Integration work will greatly depend on what your product is built using. Where existing plugins are available, you can be up and running using Digi-ID in a matter of minutes.

Where there is no existing plugin for your platform or application, we have some sample libraries that may be of use and we recommend checking out our Integration Document for Digi-ID as well as our Github: https://github.com/digibyte/

What are the security benefits as an operator and for my users?

Digi-ID can be used as an additional layer of security for your users, to compliment a traditional "Username + Password" authentication method, or alternatively as users upgrade their account and add Digi-ID you can even do away with usernames / passwords entirely.

This means end-users are unable to re-use passwords, or choose insecure passwords, if there is no "password" on their account when replaced by Digi-ID. Should a security breach occur through some other method, there would be no usernames / passwords for an attacker to obtain. It also means your users are protected from password re-use from other websites too.

How would my product work without passwords? Why would I or my users want this?

Platforms can replace their Username + Password authentication entirely with Digi-ID, giving users a Digi-ID QR Code to tap / scan to validate their identity. Login is much faster this way compared to entering credentials, not to mention you can log in to a shared PC (Such as a cyber cafe or family computing device) without worrying about your details being saved.

Each login attempt is valid only for that one session, so the 'challenge' response cannot be resent and reused for a later login attempt on a website / application.

The validation connects them to the individual "session", be it on a website, inside a mobile application, or an attempt to access building security.

This means a few things:

1. Users are proving they are "me" without any personally identifiable information
2. The weakest point of authentication, Usernames + Passwords, are removed
3. Sharing of credentials becomes far more difficult for end-users
4. Users no longer need to remember multiple sets of credentials where they use the service with more than one account (eg a home + work email login). By cryptographically proving they are who they say they are, users could associate multiple accounts with their identity.

How will I get in contact with users if there's no username / password?

Once your users are logged in, you are still welcome to ask them for an email address etc as you would currently. Same goes for a name etc, especially if you'll be shipping them a product or wanting to address your users in an email.

Digi-ID is pseudo-anonymous in so much that the only identifiable information is what they give you after the authentication request

What additional infrastructure is needed for Digi-ID to be accepted on my platform?

Digi-ID does not require you to run any additional hardware, all current implementations are fully self-contained and allow you to verify and validate users without the need for a 3rd party, or any additional servers / hardware.

Digi-ID integration libraries are able to validate an address without the need for you to even be 'online', and they don't require you to run a DigiByte server / node.