Digi-ID user 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

Why do I want to use Digi-ID?

Traditionally, to log in to a website you need to use a Username and a Password just to prove who you are. There are too many things wrong and insecure by doing this, for example:
* Users can share passwords with other users
* The passwords can be stored insecurely, both by the server or by the user (eg written down)
* Hackers can break in to websites and steal the usernames / passwords
* Keyloggers can intercept passwords
* Passwords can be reused in multiple places
* Insecure passwords can be guessed

Digi-ID does away with all of this, resulting in an exponentially more secure authentication system. No passwords to be guessed, brute-forced, stolen or written down. Digi-ID proves that you are "you", each time that you log in to a website, without the need for a username / password.

How does Digi-ID work?

The website will generate a unique QR code code for you on each visit. This QR code doesn't know who you are, or any other details. This QR code gives your Digi-ID authenticator a string of letters and numbers, along with details for where to send the login information to.

Using the same cryptographic security that keeps your DigiByte, Bitcoin and other blockchains safe + secure, your Digi-ID authenticator then encrypts the message in the QR code. This message is then sent back to the website, using only a tiny amount of data to do-so. It's very efficient.

The website then is able to take your message, along with the unique public address that you have provided to the website, and verify that you are you, and not somebody else trying to imitate you.

Why don't I need a username or password if I use Digi-ID?

Digi-ID uses advanced cryptography, that's been around for decades, to prove that you are you. Because of this, it does away with the need for usernames and passwords. This is the same security that prevents a stranger from spending your DigiByte or Bitcoin, so it's super secure.

Can't somebody just try guess my login really quickly?

Sure they can, but all the computers in the world working together would take thousands of years to guess even just one persons details, and even then it may not be the details of the person they want.

It's both mathematically and physically not plausible for a guess to happen in our lifetime or the next.

What happens if I lose my phone?

You can remotely wipe your phone, and then restore your unique passphrase to another phone or computer. Digi-ID can be used across Android, iOS, PC and Mac.

Can I use this on multiple devices at once?

Certainly! If you have a phone for work and a phone for personal use, there's nothing preventing you sharing the same details across both devices, or using a unique one for each.

Can websites see my DigiByte balance?

Absolutely not. We use a unique address just for Digi-ID that is separate from your DigiByte. In fact, a unique address is generated for each website, so that your address is not re-used.
NOTE: *You should never send DigiByte to this login address, it will not show up in your Wallet!*

How much of my personal data do you share?

We don't share anything like your name, phone-details, DOB or anything like that because even the Digi-ID authenticator doesn't know that. We don't keep any identifiable data on you, so there's nothing to send to a website when you log in. Everything is done with mathematics, cryptography and meaningless nonce's that look like this: x=458c552d84a8a347

Nothing aside from your public address is sent, and the website validates your request using unforgeable mathematics.