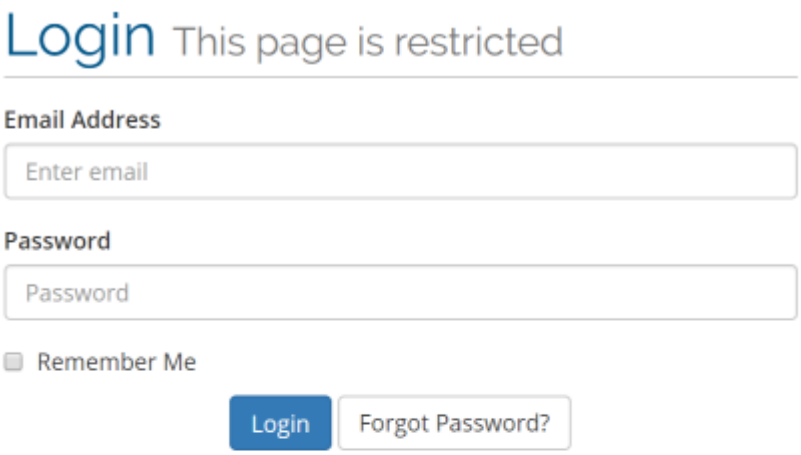
Digi-ID integration guide

Digi-ID is an open protocol that allows for fast, simple and yet incredibly secure authentication based on the DigiByte Blockchain. Digi-ID utilizes public key cryptography much in the same way keyless SSH access works, just with a user-friendly wrapper around it.

Specification

Prior to being given access to a secure / restricted area of a website or service, the user will be shown a QR code, potentially alongside existing authentication methods:



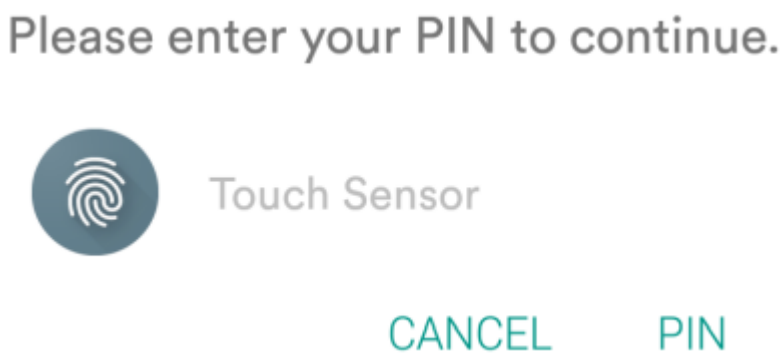
The QR code contains:

digiid://www.website.com/callback?x=NONCE

- digiid is the protocol scheme used to trigger mobile applications when tapped
- www.website.com/callback is the callback URL. https is strongly recommended.
- x=NONCE is the nonce which must always be unique and will be linked to the users session ID

http is only accepted with "&u=1" appended to the callback URL, however this is only recommended during development / testing and should not be used in production environments. Digi-ID is not a substitute for SSL encryption.

Once the QR code is scanned by the user in the Digi-ID authenticator or DigiByte Wallet, the user will be prompted to confirm authentication for the target service.



The user will then enter their unique PIN or scan their fingerprint to confirm. They will be prompted with a dialog box or toast message indicating success or an error message if applicable.

The server verifies the signature validity, then allows the user access to the authenticated session. Only the users public key needs to be kept on the server, though naturally additional information can be stored alongside as needed, though everything else is optional from an authentication perspective.

The server should also have a timeout for the nonce validity in order to prevent replay attacks.

(Do we need the info about HD wallet derivation path here, or, can that go elsewhere for Wallet integrators?)

https://github.com/bitid/bitid/blob/master/BIP_draft.md

Do you have a sample / demonstration website available?

Yes, you can try out Digi-ID at https://digiid.digibyteprojects.com

Is there a sample PHP library to help me integrate Digi-ID?

Yes, it's available at https://github.com/digibyte/digi-id-php-library

Is there a sample Javascript library to help me integrate Digi-ID?

Yes, it's available at https://github.com/digibyte/digi-id-js-library

What is a preferred time for the nonce timeout?

Depending on the application this may need to be shortened or lengthened. For most websites, a 90-second expiration is likely sufficient, in order to minimize time for replay attempts.

Do I need the DigiByte "D" in the QR code?

No, this is completely optional. We recommend prefixing the QR code with "Login with Digi-ID" in order to avoid any confusion for users.

Do I need to run a full DigiByte node to utilize Digi-ID?

There is no need to run a full DigiByte node, the PHP and Javascript libraries are a complete implementation that do not require any external connections to the DigiByte Blockchain or 3rd party service

Can this work in a WAN / offline scenario?

Yes, provided there is a way for the Digi-ID authenticator to resolve the callback URL (Such as WiFi / WAN), Digi-ID will work just fine.

How can Digi-ID be used for building access control?

A screen that generates a QR Code can be set up near a door or other restricted area. The user scans this QR code with their cellphone using the Digi-ID Authenticator or DigiByte Wallet, as they would for a website. Once scanned, this sends the encrypted message to your central building authentication server which keeps track of which QR code was scanned by each door having a unique callback URL. Your server then matches the users public address to the relevant door and if authorized it unlocks the door for the user.

Why do users get different addresses across different sites

Because the domain name is included in the hash, it means if you use multiple callback URLs (Perhaps in the building security example above), provided they all use the same domain-name then the public key generated will be the same. The protocol and the domain are hashed in when signing, but the path after the / in the URL is not used.

Can Digi-ID be integrated in to a 3rd-party wallet?

Yes, absolutely!

- URI is the callback URI and not the Digi-ID URI)
- index is a 32-bit unsigned int, which is used to generate more keys corresponding to the same URI. If not set this should be assumed "0", as it is not currently utilized in any of the DigiByte Go / Mobile wallets or Authenticators

HD structure

1. Concatenate the little endian representation of index with the URI
2. Compute the SHA256 hash of the result
3. Take the first 128 bits of the hash and split it in to 4x 32-bit numbers, A, B, C & D (each in little endian notation)
4. Set highest bits of numbers A, B, C & D to 1

5. Derive the HD node m/13’/A’/B’/C’/D’ according to BIP32

Testing

BIP39 seed: myth glimpse mystery abstract embark net faint hospital catch hint develop state

Callback URI: digiid://digiid.digibyteprojects.com/callback?x=c6140375e5bae71e

Index: 0

Hash result: 460ebbfd1df7410106d62d41f802f769bc00db825e9cf8c649cb069dec35e8fb

BIP32 path: m/2147483661/4256894534/2168583965/3241006598/3925279480

Digi-ID address: DJDAkjie6nrW6RpFZSTpNUXsZ9JE2x6p1o