MATTR GO

Product Specification Sheet

WHITE LABEL WALLET APPLICATION

WALLET CAPABILITIES*

V1.0.8

Overview

The MATTR GO Wallet application provides customers with a fast and convenient way of creating a white-label branded wallet for use in their credential ecosystems.

MATTR's base wallet application is backed by user testing and research, giving end users a world class wallet experience. The white-label MATTR GO Wallet application leverages all the benefits of the base application but allows customers to wrap the interface in a brand their end users already know and trust.

It is suitable for customers looking for a "ready to use wallet" that can be distributed directly to holders of credentials in their ecosystem, with no coding required.

The MATTR GO Wallet is designed for use with MATTR's credential lifecycle capabilities, available in the MATTR V// Platform.

Features

The MATTR GO Wallet supports the following key features:

- Collect credentials from issuers
- Present credentials to verifiers
- Custom branding of the wallet user interface
- Multi-language support with option for additional local languages
- Cross-platform support as referenced in MATTR Learn
- Receive access to the latest UI/UX and specification updates**

*MATTR GO Wallet capabilities can be packaged with MATTR V// or MATTR Π capabilities. Contact us for more information on available packages, pricing and language pack support.

**The MATTR GO Wallet is distinct from other MATTR wallet capabilities and may not follow the same update and maintenance cycles as any other MATTR wallet capabilities or showcase applications.

Note: All MATTR GO Wallet capabilities require a one-off set up service (fees apply), which includes configuration, branding and other setup activities by MATTR team members.

Functionality

Scan, tap or click to obtain and present credentials – enable users to be issued credentials or share credentials for verification with a QR code or a deeplink.

Utilise biometric authentication – use local device authentication features to access the wallet (facial recognition and fingerprint).

Receive messages and push notifications – wallet users can enable push notifications to start an action, such as a verification flow.

Collect and present credentials using multiple protocols – issue and present credentials in the wallet using OpenID4VCI and VP Request specifications.

Enable high assurance authentication and binding – create high assurance verifiable presentations based on cryptographic authentication factors.

Preserve privacy with selective disclosure – some credentials can reveal only relevant information when presenting them to verifiers in certain contexts.

Keep a record of activity – a dedicated activity tab allows users to see an audit log of interactions with specific issuers and verifiers.

Create trusted interactions – domains of issuers and verifiers are validated using DID-to-Domain credentials. If successful, a verified tick is shown during the flows.

Support display of custom-branded credentials – allow issuers to add custom logos, colours and watermarks to their credentials.

Customise wallet user interface and Ts&Cs – choose colour, text, fonts, custom imagery and more using design tokens. Plus, include your own terms and conditions.

Choose your wallet language – the wallet supports multiple base languages, and there is the ability to expand support for additional language packs.

Deploy under your own publisher account - publish your wallet app under your own app store account using your app signing keys.