

What is needed to Trust a Wallet App?



Wallet Attestations for
now and the future.
User Choice of Wallet

Six Trust Vectors (from our previous Workshop)



1. Issuer Trusts Wallet

To approve endorsing and provisioning credentials for its Users into that Wallet, Cloud Wallet, Login system



2. Reader Trusts Wallet

To establish that credential protection was achieved and User Authentication actions can be trusted.



3. User Trusts Verifier

To give informed consent and approve sharing their data to the expected Reader or Website. And **not** to violate their privacy expectations for the transaction.



4. Reader Trusts Issuer

To validate received credential data (from wallets, cloud wallets, or login systems).



5. Ecosystem Trusts Reader

The Reader or Website, on behalf of a Verifier, can properly identify itself to Users to make a data request with the purpose for that request.



6. User Trusts Wallet

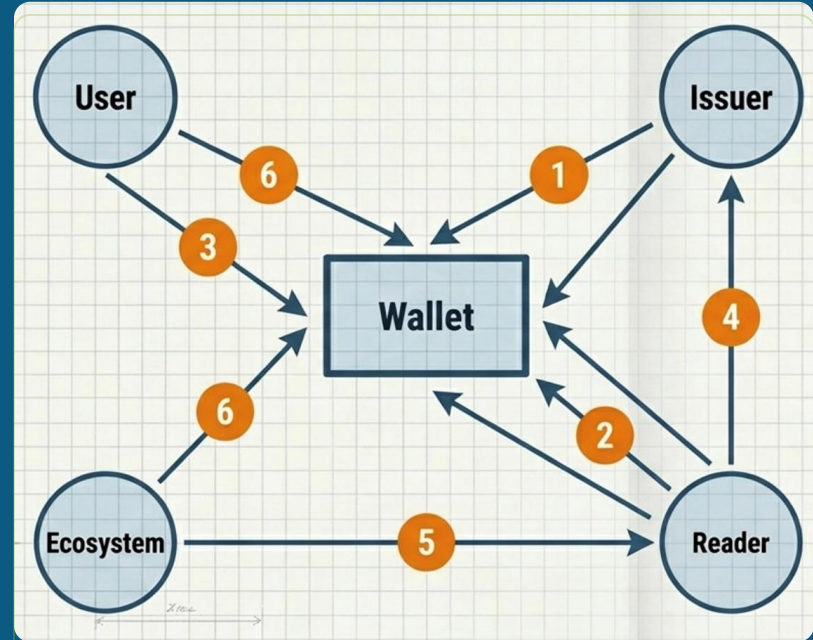
Wallet will work everywhere, securely store their receipts, secure their ID, not profile their transactions, and not exceed the bounds of privacy expectations.

Wallet at the Center

(App, Platform, Hardware, or Cloud Wallets)

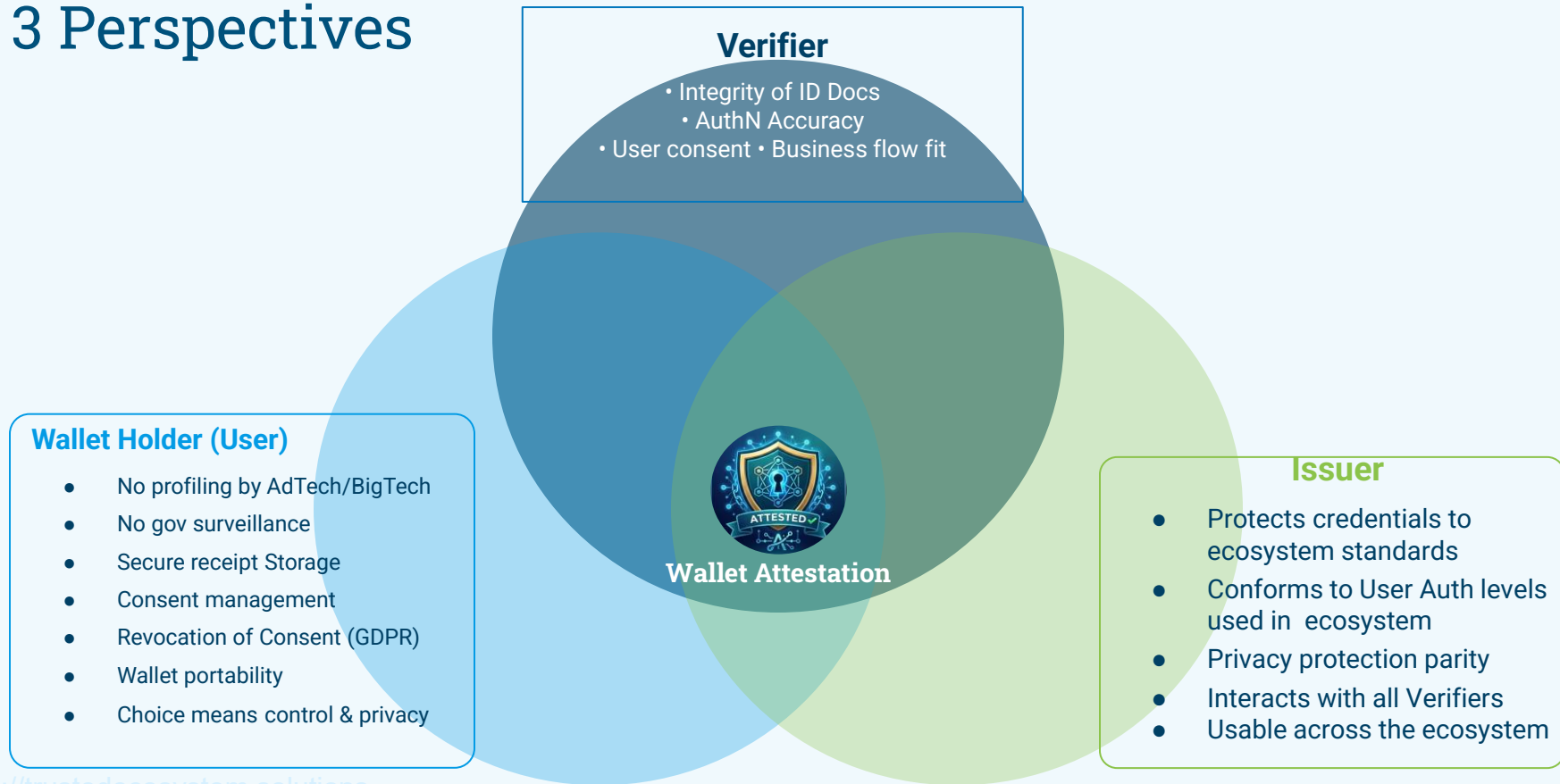
When you redraw our Trust Vectors, you realize how much the wallet is **core to trust**

Trust Vector Flows



Potential Requirements on a Wallet

3 Perspectives



Wallet Attestations need to show that the wallet instance can:

- Protect and Update the Credential
- Perform User Authentication to a Credential
- Meet Privacy Expectations of the User
- Meet Ecosystem Requirements

