OWF Privacy and Consent

Proposal to OWF technical architecture
From Tom Jones 2023-07-17

Consent Considerations

Any initial message to a wallet from a website must include this information:

1. Consent applies to the human holder of wallets that contain subject private data
2. The initial message from the website must be signed
3. The signer of the message must be identified
4. There must be sufficient ID information to display to the holder for trust
5. The purpose of any request must be clearly displayable to the holder
6. The impact of any user choice must be clear to the holder
7. No data can be sent from the wallet without a user gesture of consent
    a. That means no permanent identifier information about the wallet or device as well
    b. This applies to all messages from the device that can be tracked
8. In general most requests for data will be displayed on a single page
    a. A single page is the most that the majority of holders will tolerate
    b. That page must be sufficient for the holder to accept or reject consent

Privacy Considerations - General

1. The holder of the wallet has complete control over all private data
    a. If any sovereign request for data is executed, the holder must be informed
2. No information supplied by the wallet may enable tracking w/o consent
    a. Including device of behavior tracking
3. Transactions or Receipts from websites are private data in the wallet
4. A threat analysis is required of all wallets for privacy considerations
5. Biometric data that is used by the wallet to identify the user is not sent
    a. But it is possible for a verifier to ask for biometric data if that is germane
6. What is displayed will be moderated by the holder’s settings for the wallet

Privacy Considerations - Issuer

1. If the Issuer requires user identifiers, trust must first be established
2. The holder information should be limited to what is required to get the cred
3. Issuer may verify the holder or the holder presence at any time (see below)
4. For high risk data the issuer should assure the wallet can protect data
    a. At a minimum this would include health and finance data
5. Whatever information is provided by the issuer must be:
    a. Protected from disclosure
    b. Enable selected disclosure if more than one element is provided

Privacy Considerations - Verifier

1. Proof of presence information can be obtained by the wallet as requested
    a. Liveness and holder verification
2. If any user data is required by the verifier, it must be identified
3. The verifier must be clear about data requested and retained
4. Some jurisdictions require that optional data be separately identified
5. The verifier must inform the holder as to all parties processing data
6. Some verifiers may request wallet assurance that data is protected
7. It should be possible for the holder to see the detailed data request
8. It should be possible for the holder to see terms and conditions
9. If the holder is a delegate for the subject, proof of authority may be required

Taxonomy and Notes

- Wallet = User Agent that can securely store and use holder’s secrets
- Device = A mobile computing device with wireless network access
- User data = Personally Identifiable Information
- Credential = Immutable signed data given to the wallet to store and use
- Holder = Natural human that has installed the wallet on the mobile phone
- Subject = Natural human that holds sovereign control of data about themself
- Tracking = Any process that allows any service to aggregated subject data
- Privacy within the wallet has not be addressed in this presentation
    - It is unclear if that topic is to be addressed by this group

Resources - Privacy and Consent

- Mobile Privacy Experience - Tom Jones
- Report on mobile Driving License Privacy - Kantara
- Government-Issued Digital Credentials and the Privacy Landscape - OpenID