Safe Wallet Analysis Framework

v0.951

26th March 2024

Revision History

v0.951	26th Mar 2024	Added EU Digital identity Wallet example to the Holder Binding Section	Dan Bachenheimer
v0.95	25th Mar 2024	Updates following further reviews.	Andy Tobin Juliana Cafik Jorge Flores Keith Kowal
v0.91	25th Feb 2024	Incorporated external feedback from Jamie Smith++. Multiple refinements & clarity edits.	Dan Bachenheimer, Juliana Cafik, Jamie Smith, ++ Andy Tobin
v0.9	15th Feb 2024	Incorporating feedback from OWF Government Advisory Council and external reviewers	Andy Tobin Sankarshan Mukhopadhyay
v0.8	6th Feb 2024	Updates to Wallet/Device Lock/Unlock Updates to Security	Tim Bloomfield Juliana Cafik
v0.7	30th Jan 2024	Updates to Holder Binding and Certification sections to change questions into requirements.	Andy Tobin
v.06	23rd Jan 2024	Updates to Security section Updates to Holder Binding section	Juliana Cafik Andy Tobin & Tim Bloomfield
v0.5	16 Jan 2024	Multiple updates	Daniel Bachenheimer Tracy Kuhrt Tim Bloomfield
v0.4	9 Jan 2024	Updates for consistency & flow. Acceptance of multiple prior changes.	Andy Tobin
v0.3	5 Dec 2023	Updates for consistency & flow. Additions for clarity & new content.	Daniel Bachenheimer
v0.2	Various	Multiple updates and additions into each section.	Andy Tobin Juliana Cafik Sebastian Elfors Stavros Kounis Tracy Kuhrt Juan Francisco Tavira Lal Chandran Daniel Bachenheimer
v0.1	22 Sep 2023	Initial framework	Andy Tobin

Contents

Introduction **3**
Background **3**
Purpose **4**
Audience **4**
Scope **5**
How to Use This Analysis Framework **5**
Categories **6**
Analysis **6**
Important Note on the Analysis Approach 6
Privacy **7**
Security **10**
Trusted Processes: 11
Security Design Controls & Considerations: 13
Wallet & Device Locking and Unlocking Mechanisms **15**
Holder Binding **17**
Additional information regarding biometrics in holder binding 19
Regulatory Compliance **20**
Certification **21**
User Interface / User Experience **22**
UI/UX rules 22
Resources and References 23
Counterparties **24**
Audit **25**
Accountability **25**
Checklist for Technical Accountability Mechanisms 26
Checklist for Governance Accountability Mechanisms 26

Introduction

Digital wallets promise to revolutionize the digital interactions of businesses, governments, and people. However they are still relatively new, evolving very quickly, and utilize sophisticated cryptographic mechanisms. Demand is increasing, and new digital wallets are being brought to market all the time.

Yet many aspects of the functionality, design and implementation of digital wallets remain complex and hard for non-experts to understand.

This is a concern when increasing parts of our digital lives are becoming dependent on digital wallets for day-to-day activities. How does an average user know if their wallet is safe to use? How does a journalist accurately report on the privacy or security features of different wallets? How does a policy maker pick through the technical complexities of competing wallet platforms to determine which are safe for citizens?

To address this concern, the OpenWallet Foundation (OWF) Safe Wallet Special Interest Group (SIG) has prepared this framework and the accompanying analysis template. Our goal is to provide a way for analysts to create simple and easy-to-understand comparisons of the safety features of different digital wallets that can be appreciated by non-experts. IMPORTANT: This framework is not intended to replace a formal certification process such as would be carried out by an accredited body.

Background

Digital Wallets put the holder in control of their digital assets (e.g., identity information, financial instruments, other tokenized assets) and can provide a means to verify digital credentials. Unless they are implemented carefully, they can open new vulnerabilities, such as security flaws or "back-doors" for undesirable surveillance, profiling, fraud, and the active correlation of users.

This is especially the case when previously closed and tightly controlled digital interactions are conducted in much wider and larger scale open ecosystems, where control over every possible use case cannot be exerted by a single body. Such larger open ecosystems include national and international scale wallet ecosystems that are actively developing in order to take advantage of recent advances in digital credentials.

Due to the technical complexities of the cryptography and protocols used, there are a limited number of people that understand what these vulnerabilities are and how to mitigate them.

There is a danger that implementers of well intentioned wallet initiatives, deployed at scale, may find that they have unknowingly created problems that may reduce or destroy trust in the ecosystem they are fostering if vulnerabilities like user profiling and correlation becomes commonplace. A good example from the Internet is the cookie. Initially implemented as a simple way to store items in an online shopping cart, they have morphed to become one of the most powerful user tracking and surveillance tools in history.

To address this issue, and foster collaboration, clarity and openness in the digital wallet industry, the Open Wallet Foundation created the Safe Wallet Special Interest Group in 2023. A group of the digital wallet experts came together in this group to create this framework, spending many months determining what criteria to use, how to simplify the output using ten categories, and how to handle different use cases and contexts. The result is this framework and the accompanying analysis template.

Purpose

To minimize implementation risks when deploying digital wallets, this framework introduces the reader to a range of potential vulnerabilities associated with digital wallets, and the credential ecosystems they work within, and how to avoid them.

It will also provide a means to analyze how "safe" the new breed of digital wallets is and be able to compare them effectively.

It is recommended that independent 3rd-party analysts are utilized for carrying out comparative analysis to avoid potential bias when self-assessment is carried out by wallet developers themselves. This does not preclude self-analysis, but readers of the resulting output should be made aware of who has carried out the analysis.

The provision of the optional companion analysis matrix will enable like-for-like comparisons of digital wallets in a simple and easy way.

Different use cases and contexts will have very different demands on digital wallet capabilities, so readers should note the instructions in the analysis matrix and take this into account in their analysis. Similarly, the standards, technologies and protocols used by different ecosystems will have a significant impact on the capabilities of digital wallets operating within those ecosystems which analysts need to take into account. Weightings can be applied to the analysis criteria to handle use-case and ecosystem specific differences and the importance of various criteria in a specific wallet ecosystem.

Note that this framework does not replace a formal assessment by an accredited body.

Audience

The goal of this framework is to inform its readers about what “safe” looks like **for their specific use case(s)**.

There are two primary audiences for this framework:

- Those wanting a simple to understand comparison of the safety of digital wallets.
    - This audience is likely to be legislators, politicians, journalists, members of the public, and advisors. People that are not deeply involved digital wallet experts, but want to know and understand more about them and their implications.

    - These people will have read a comparison between digital wallets' safety scores and be looking for more detail about the analysis method and different categories making up the scores.
- Those wanting to analyze or create a comparison of digital wallets' safety criteria.
    - Analysts, consultants, and subject matter experts can use this framework and the accompanying analysis template to create comparisons of the safety levels of different digital wallets. The information contained herein provides information (and links to further detail) for such comparisons to be conducted, and a consistent way to present the output.

It is anticipated that wallet developers, consultants and other experts in the field of digital wallets and credentials will use this framework and adapt it in their own work, and the authors note that they are entitled to their own opinions on the importance of the various categories described in this framework and ask them to contribute to future versions of this framework.

Scope

The focus of this framework is to assist the reader in assessing how safe a digital wallet is relative to other digital wallets for a variety of identified use cases in a targeted credential ecosystem.

By necessity, the scope also extends to other participants in the digital wallet ecosystem who have a significant impact on the deployment and use of digital wallets, including the issuers and verifiers of credentials, the developers and providers of wallets, and those who set up governance frameworks for wallet use.

This framework does not itself seek to rank or compare different digital wallets. Its purpose is to provide a methodology and direction for others to create such comparisons in a consistent and meaningful way.

How to Use This Analysis Framework

This document contains considerations in the form of requirements and recommendations. It splits up the complexity of digital wallet ecosystems into ten categories for simplicity, and gives guidance on the best practice in those categories.

It is not the equivalent of a product requirements definition document but could be used as input for one.

Different digital wallet ecosystems will need different capabilities. It is beyond the scope of this framework to cater to every different use case, therefore it is up to the user of this framework to factor in the relative importance (weight) of each functional category for their use case and ecosystem. This should be stated clearly in the resulting analysis to ensure that readers are clear what choices have been made when creating the comparison.

Users of this framework that are conducting comparison exercises should first determine the use case(s) and contexts for the digital wallets they wish to review. It is desirable to compare like-for-like to get meaningful output, but it is up to the user of this framework to determine what they want to compare.

Please see the implementation notes in the accompanying analysis template.

For those looking at the output of a digital wallet comparison performed by someone else, this framework can be used to examine in more detail the requirements or functionality in any of the 42 sub-categories

Categories

The framework defines ten categories and 42 sub-categories that can be used to analyze any digital wallet from a safety perspective.

The ten categories are:

1. Privacy
2. Security
3. Wallet & device locking and unlocking mechanisms
4. Holder binding
5. Legislation compliance
6. Certification
7. Accountability
8. User Interface / User Experience
9. Counterparties
10. Audit

Analysis

To enable easy comparison of different digital wallets, this framework introduces an optional analysis template (see separate spreadsheet) that can be used to compare digital wallets across the different categories.

The intention is to provide a mechanism that produces easy-to-read comparative analysis that can be quickly understood, and also provide the means to examine each wallet in more detail to understand how the analysis has been arrived at.

Important Note on the Analysis Approach

Users of this framework should be aware that it is important to view any safe wallet analysis within the context of the use of the wallets that are being analyzed. Therefore a low score in one category may be fine for the given context. Users of this framework should be careful to ensure that they are aware of the intended use case or context for digital wallet use to avoid creating inaccurate or unrealistic comparisons.

As an example, a digital wallet that is used primarily in a closed system for employee ID and login will have different requirements than a digital wallet used in a completely open ecosystem spanning hundreds of possible use cases and many thousands of issuers and relying parties. Similarly, wallets that carry out the same job but use different underlying technical approaches (e.g. anoncreds versus mDL) will have different relative scoring which will be important for analysts to note.

To handle this context sensitivity, the accompanying spreadsheet includes a weighting function to allow analysts to set up their analysis according to the relative importance of different factors in the ecosystem, context or use case that they are examining. This will enable analysts to handle the fact that one ecosystem may have a much higher emphasis on (for example) privacy, than another.

The intention is that this analysis method is used for complete wallet applications. Open source wallet components can require special treatment due to the way that their code can be incorporated into 3rd party wallet apps, and the level of examination required to determine if the developers (possibly many loosely connected people) have created the code in a way that satisfies the rigor and robustness required.

Privacy

In the context of digital wallets, privacy primarily relates to how a user's activities are protected from unwanted observation, tracking and correlation.

Digital wallets and the digital credentials they manage, along with the protocols involved in their issuance and verification, introduce a new set of challenges that don't exist in the world of physical (paper and plastic) credentials.

- Unique Identifiers.
  - Holder-specific or wallet-specific unique identifiers that may be shared, without holder choice, with every transaction must be avoided.
    - Such identifiers are akin to a tracking beacon that allows colluding entities to correlate all activities of a holder using that wallet.
    - This is particularly dangerous when proxy verification services are used, that process verifications for many relying parties and will be able to see and track such an identifier and profile the behaviors of all holders.
    - An example of such an identifier is a wallet serial number in the "metadata" of the credential exchange transaction.
    - Although not necessarily wallet-specific, the exposure of IP addresses used in digital interchanges should be factored into the overall operational risk profile
  - Credential-specific unique identifiers that are shared, without user choice, are another class of unique identifiers that should be avoided.

        - While not as privacy impacting as a holder or wallet-specific identifier because it isn't necessarily shared with every transaction, a credential-specific identifier that the user cannot avoid sharing will enable transaction correlation whenever that credential is used.
        - An example of a credential-specific identifier is a revocation index position or an issuer signature in the "metadata" of the credential exchange transaction.
        - Another example of a credential-specific identifiers may come in the form of payment credentials which may contain unique identifiers for compliance within the financial services industry
        - A useful comparison of different credential types has been carried out by Andre Kudra, Torsten Lodderstedt, Paul Bastian, Mirko Mollik, Maaike van Leuken, Caspar Roelofs.

- Decoupling issuers and verifiers.
    - Digital wallets and their associated ecosystem(s) should prevent issuers from being able to track where, when, or with whom holders use their digital credentials.
        - Issuers and verifiers of digital credentials should not be able to track their use which would enable them to, for example, build user profiles. However, transactions where usage tracking is a fundamental part of the use case that holders are fully aware of (payments being an example) would be accepted in that context.
        - Issuers should not be able to aggregate holder information.
        - Verifiers should be prevented from contacting issuers (decoupling) for any reason including to check the revocation status of digital credentials. If decoupling is not implemented, issuers could track the use of digital credentials they have issued. This is known as the "phone home" problem.[1]
            - Phone home architectures should not be used.
            - Back-channel interactions between verifiers and issuers that are not visible to holders should not be used.
        - Verifiers should check the authenticity and integrity of each issuer-signed credential to determine whether to trust it.
        - Verifiers should not be able to access any digital wallet contents without holder consent
- Wallet support of privacy preserving credential sharing mechanisms
    - The wallet must support privacy preserving credential mechanisms that, for example, ensure that only a set of data attributes within a credential need to be revealed rather than the entire credential (such as providing just a first name and photo from a driving license rather than all the data in that

[1] Decoupling is not a digital wallet specific vulnerability but the authors felt it imperative to call it out in context of digital wallet usage.

license), and proving possession of data without revealing the values of the data itself (such as an over-18 age check without revealing date of birth).

- This can be achieved using techniques such as selective disclosure, calculated or predetermined predicate proofs. and zero-knowledge proofs.

- Wallet transaction privacy.
    - The code providers and/or cloud operators of digital wallets must not be able to observe or track transactions undertaken by holders.
        - This is particularly important in the case of hybrid and pure cloud wallets, where transactions are performed on the wallet operator's infrastructure.
        - Wallet code providers and cloud operators must not be able to access the contents of digital wallet transactions or backups.
        - Wallet code providers and cloud operators must not have a "master key" that enables them to access the contents of wallets that they have custody of.
- Digital Wallet ecosystem providers.
    - Organizations that provide the infrastructure to which digital wallets connect in order to issue or verify credentials (typically called credential exchange platforms) must not be able to examine the contents, source or destination of wallet transactions.
        - In many situations, such credential exchange platforms will need to "translate" from an encrypted credential envelope to/from clear text for integration with other systems, such as customer onboarding systems.
        - In this case, the credential exchange platform must manage the data in such a way that it is transient and not stored, observable, or trackable to protect wallet holder privacy.
    - Proxy services may provide credential issuance/verification services for many issuers and verifiers. In doing so, they could observe and correlate wallet transactions across large ecosystems.
        - Proxy services must not observe, store and correlate wallet transactions.
        - Holders should be informed that they are dealing with a proxy service rather than the true end issuer/verifier.
- Consent Management
    - The wallet must provide clear, understandable and easy-to-use mechanisms for the user to provide consent to add data or read data from their wallet. This is a major privacy consideration and ensures the user is in control of their data.
    - Users must be able to track the consent that they have given and be able to withdraw that consent at any time.
    - The act of provision of consent by the user should not itself leak personal information. For example, apps based React Native framework commonly make use of this open-source npm package https://www.npmjs.com/package/react-native-device-info which exposes

sensitive information such as unique device identifier, device type and brand etc. A unique device identifier may be classified as PII under certain jurisdictions such as CCPA.

Security

At its most basic, a digital wallet is a holder-controlled digital container sitting between Issuers of verifiable credentials and a Verifier and/or Relying Party that authorizes access to, and the provisioning of, services.

A digital wallet is a critical confluence point in a credential-based interaction and must be able to establish, maintain and attest to the trusted processes required for a trustworthy, secure and safe digital transaction. Please refer to the OWF Architectural SIG[2] for more information on this matter.

According to the European Union[3], a compliant EU digital wallet *will provide a secure and convenient way for European citizens and business to ****share identity data **** needed for accessing digital services such as checking in at the airport, renting a car, opening a bank account, or when logging in to their accounts on large online platforms.*

Digital wallets are instrumental to the acquisition, storage and presentation of credential-based assertions, and the security of wallets is essential to safeguarding the integrity and privacy of those assertions. Wallet architecture should consider security by design and Zero Trust security best practices with a focus of least privilege for applications. Wallet components should correspondingly be based on robust security controls capable of providing evidence to the context, methodology, and strength of the controls as well as confirm their authenticity and state while in use. Wallet security controls must also mitigate risks from evolving attack surfaces and vectors on consumer devices, to detect potential vulnerabilities such as (but not limited to) phishing attacks, man-in-the-middle, relay attacks, malware and lost or stolen devices.

The Digital Identity & Authentication Council of Canada's (DIACC's) Digital Wallet Component Conformance Criteria states: "The integrity of a Trusted Process is paramount because many Participants may rely on the output of the process, often across jurisdictional, organizational, and sectoral boundaries."

The DIACC's Digital Wallet Conformance Profile[4] also includes a comprehensive breakout detailing the Type of Risk, Threat Category, Impact and Proposed Mitigation, which is a good example of what and how to assess digital wallet conformance to these critical design elements.

[2] https://github.com/openwallet-foundation/architecture-sig/blob/main/README.md

[3] https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox

[4] https://diacc.ca/wp-content/uploads/2023/04/PCTF-Digital-Wallet_Conformance-Profile-Final-Recommendation-V1.0.pdf

Expanding on the foundational work that DIACC has done, this document describes Trusted Processes and Security Design Controls & Considerations that may be necessary to provide safety for wallet holders as well as meet the required levels of assurance for issuers, verifiers and relying parties and provide an awareness of state via attestation for:

Trusted Processes:B

- Wallet Selection: Wallet selection refers to the process of the user or device operating system choosing a digital wallet for a specific purpose while ensuring optimal security and safety. In a situation where multiple wallets are available, a wallet selector is an additional step in the wallet user flow when sending or receiving transactions, to prompt a provider to choose the specific digital wallet they wish to use for a specific use-case. The goal is to select a wallet that not only provides convenience but also ensures safety and security for all interactions on an ongoing basis. This is fundamental to the establishment of trust, the assurance of privacy and the efficacy necessary to create a positive and adoptable wallet-holder experience. Wallet selection can pose several security risks and considerations for prevention include (but are not limited to):
    - Malware:
        - Regular Software Updates: Continually update wallet software, operating systems, internet browsers, phone firmware, and antivirus software to fix known vulnerabilities as they are discovered
        - Secure connections and end-point management for all network interactions, including NFC and Bluetooth low-energy enabled hardware
        - Phishing resistant authentication
        - Obtain wallet software from official sources
        - Root detection for mobile devices
    - Social Engineering prevention involves a combination of technical measures, policy enforcement and wallet holder education. Strategies for mitigation include:
        - User Education: Users should be educated about the common tactics used in social engineering attacks and how to identify potential scams.
        - Phishing resistant authentication
        - End-point security
        - Regular audits of accounts and access levels
        - Software updates to prevent evolving known vulnerabilities
        - Policy enforcement for policies and procedures that consider potential social engineering vectors and provide specific guidance on steps to take to avoid successful attacks
    - Brute Force Attack Mitigation options:
        - Phishing resistant authentication
        - Account lockouts and rate limiting
        - Strong data encryption & storage

  - End-point authentication to prevent:
    - Man-in-the-Middle Attacks such as:
      - Relay Attacks: relaying information between parties
      - Replay Attacks: Capturing and reusing information
- Key Management: this is an essential function involving the handling and safeguarding of cryptographic keys to ensure the security and integrity of the holder's digital assets. Primary security considerations and controls for key management are:
  - Storage: Keys must be stored securely to prevent unauthorized access.
  - Key Generation
  - Backup and Recovery: A robust key recovery system, or process, is critical to ensure users are able to regain access to their wallet(s)if the private keys are lost or compromised.
  - Usage: Keys must be protected while in use in a secure manner & within a secure environment
  - Key Rotation: The process of changing keys to maintain integrity and security
  - Key Revocation: The process of revoking and replacing compromised keys
  - Audit: Processes for logging and detecting security risks to keys.
- Credential Signature / Format: A credential signature in the context of a digital wallet is a digital proof that verifies the authenticity of the credential. For a secure credential signature, it is important for the wallet to support:
  - Credential Signature Verification: mechanisms to verify the authenticity of the credential signatures to ensure they have not been tampered with and are issued by a legitimate trusted authority
  - Secure Storage of Credentials: Secure storage to prevent unauthorized access and tampering with verified signatures
  - Privacy Preservation: Mechanisms to support the verification of credentials without revealing of unnecessary personal information, such as selective disclosure and zero-knowledge proofs.
- Credential Management: Credential management in the context of a digital wallet refers to the process of handling and safeguarding digital credentials to ensure their integrity.
  - Storage: Credentials must be stored securely to prevent unauthorized access.
  - Backup and Recovery: A recovery system, or process, to ensure holders are able to regain access to their wallet(s) if their credentials are lost or compromised.
  - Usage: Digital wallet architecture must support credential use in a secure manner & within a secure environment
  - Revocation: The process of revoking and replacing compromised credentials
  - Audit: Processes for logging and detecting security risks to credentials.
- Presentation Protocols: Presentation protocols in the context of a digital wallet refer to the standardized methods for presenting, sharing and verifying digital credentials. The protocols ensure interoperability and secure communication between different entities in the digital ecosystem, include standards-based

credential presentation and verification and are crucial to the security and privacy of a holder's digital identity. To preserve the integrity of presentation protocols several wallet security measures must be implemented:

  - Phishing-resistant user authentication to ensure the holder presenting the credentials is the legitimate holder of both the wallet and the credential
  - Secure, Phishing and 'spoof' resistant user interface
  - Strong data encryption and storage to secure credentials and prevent unauthorized access
  - Digital wallet user interface and architecture to support credential presentation and usage in a secure manner
  - Privacy-preserving mechanisms to support the presentation of credentials without revealing unnecessary personal information, such as selective disclosure and/or zero-knowledge proofs
  - Audit processes for logging and detecting security risks, such as malware, phishing attacks, man-in-the-middle attacks, etc, that may impact credential presentation.

- Mechanisms to convey consent: User Consent is a critical aspect of privacy and security in digital wallets. It provides credential holders with control over wallet interactions and the sharing of specific information, such as credentials with a service provider. To support secure holder consent, the following mechanisms should be implemented:
  - Phishing-resistant user authentication to ensure the holder providing consent is the legitimate holder of both the wallet and the credential
  - Phishing and 'spoof' resistant user interface
  - Strong data encryption and storage to secure sensitive data and consent records and prevent unauthorized access
  - Revocation mechanism to provide holders with the option to revoke consent such as a protocol for sending the revocation to the relying party, and a regulatory framework for requiring the relying party to act upon such revocation.

Security Design Controls & Considerations:

- Security by design: Implementing secure by design strategies throughout the software development lifecycle to enhance security outcomes. These approaches aim to improve collective security by incorporating security considerations throughout the software development life cycle. In the context of open-source digital wallets, these strategies are essential for advancing collective security. By implementing secure by design principles during the design phase of product development, the number of vulnerabilities that can be exploited by adversaries can be minimized:
  - Zero Trust: assumption of breach requiring verification of each request
  - Open Design: the security of a mechanism should not depend on the secrecy of its design or implementation
  - Attack surface minimization: a security strategy that aims to reduce the number of potential vulnerabilities in a wallet by limiting the ways in which it

    can be attacked. This can be achieved by reducing the number of entry, end points and APIs and by limiting the functionality and access of the wallet to only what is necessary for its intended purpose. By minimizing the attack surface, the wallet becomes more difficult to compromise, as there are fewer ways for an attacker to gain access or exploit vulnerabilities.
    - Defense in depth: a security strategy that employs multiple layers of protection to slow down or prevent an attack from gaining unauthorized access to information. Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure.
    - Least privilege: a security concept that requires each user, system, or process related to the wallet to have a minimum level of access necessary to perform its function. This means that users, systems, or processes should only have access to the resources and information related to the wallet that they need to do their job, and nothing more. This approach helps to reduce the risk of unauthorized access or malicious actions, as it limits the potential damage that can be caused if a user, system, or process is compromised
    - Need to know: a security concept that states that access to information should be restricted to individuals who require that information to perform a specific task or function. This means restricting access to the information that is necessary for them to complete a task, and no more. This principle is closely related to the principle of least privilege, By following the need-to-know principle, wallet developers can reduce the risk of unauthorized access or disclosure of sensitive information
    - Role Based Access Controls (RBAC): is a method of regulating access to resources based on the roles of individual users. In RBAC, permissions are assigned to roles, and users are assigned to roles. This allows for access to be restricted based on function, such as wallet Holder, Software Developer, Quality Assurance (QA), Project Managers, Security Analysts, and System Administrators, with roles being broad for general access or fine-grained to restrict specific capabilities.
    - Separation of Duties: a security principle that shifts the burden of security as much as possible away from the end-user, or holder in the context of a wallet, to the wallet developer(s). This principle is based on the idea that no single individual should have complete control over a critical process or system, and that by distributing responsibilities and privileges, the potential for abuse or misuse is reduced. Separation of duties is often implemented through role-based access controls (RBAC).
- Secure by Default: is a principle aimed at shifting the burden of security as much as possible away from the end-user (or holder) back to the wallet developer(s). Essentially it is about designing wallets that require minimal hardening and are secure when deployed. In the context of digital wallets this is much harder to do than secure by design, as each wallet holder’s environment is different. What works well for one wallet architecture might not work for another. It is also important to consider that secure by default features go through rigorous testing and periods of customer feedback to ensure benefit to the largest number of end users possible.
- Software Security Controls: such as NIST 800-53, are safeguards, or countermeasures, prescribed to meet a set of defined security requirements.

Controls are designed to address specific needs as specified by a set of security requirements. They aid in protecting the integrity of systems that support the wallet, involve flaw remediation, malicious code protection, system monitoring and software integrity and include:

  - Management Controls: security controls that focus on the management of risk and the management of information system security.
  - Operational Controls: controls that are primarily implemented and executed by people (as opposed to systems).
  - Technical Controls: security controls that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

- Software Bill of Materials (SBOM): An SBOM is a key building block in software security and software supply chain risk management. It provides transparency into all constituent parts of the software, which is crucial for understanding exactly what has gone into the software that is being distributed and used for the wallet. The specifics of what is included in an SBOM can vary depending on the software in question, however it should be regularly updated with details including:
  - Names of components
  - Versions
  - Licenses
  - Component relationships and dependencies
  - Third party libraries, artifacts, scripts and package versions
  - Catalog of all the software in an application including deeply nested

Wallet & Device Locking and Unlocking Mechanisms

A safe digital wallet will provide a secure and user-friendly means through which an authorized user may unlock and lock it to minimize fraudulent use. While these lock/unlock mechanisms fall into the categories of security and UI/UX, the authors feel that it is important to highlight them here, separately. It is also important to differentiate wallet lock and unlock requirements, which are typically driven by the wallet provider, from user authentication requirements, which are typically driven by the requirements of relying parties - although they may utilize similar technologies.

The mechanism and controls[5] to lock and unlock a wallet are dependent on the level of assurance (as defined by issuers and verifiers of credentials) of the wallet and the sensitivity of the data that the wallet will store.

- At a minimum, the wallet must require a PIN or password to access sensitive information including, but not limited to, personal identifying information (PII) and personal health information (PHI).
- For mobile wallets, the wallet security mechanism may be tied to the device security mechanism, such as a device PIN/Password or biometric. In addition, device biometrics (fingerprint/FaceID) may be used to bypass a PIN/Password.

[5] Note related ongoing work on ISO/IEC 23220-5

Consideration should be given to the possibility of the device holder switching off device-specific security completely.

- A wallet (web/mobile) may use an external authenticator as part of the wallet unlock mechanism.
- For medium or high assurance wallets a PIN/Password must adhere to complexity rules to reduce the possibility of guessing the PIN/Password. For example, minimum lengths, no patterns or dictionary words. In addition, the wallet user should have a limited number of attempts to enter the PIN/Password with increasing timeout delays (rate limiting).
- High assurance wallets must support multi-factor authentication - e.g., Biometrics, hardware cryptographic authenticators, password/PIN and OTP schemes

Once unlocked the digital wallet must include additional controls to protect the privacy of user data and maintain the appropriate level of security of the wallet. The following is a minimal list of controls specific to wallet lock and unlock.

- The wallet locks if focus is lost.
- The wallet locks after a pre-defined period of inactivity.
- On mobile devices, application thumbnails (displayed during app switching or selection) are blank or otherwise rendered unreadable to protect sensitive information.
- The wallet must properly secure the PIN/Password and must not persist the PIN/Password in memory after an authentication event.
- Authentication events may be triggered during sensitive operations such as displaying credential data, presenting a credential, changing a password/PIN, or operations that support holder binding requirements. The authentication event may use the default wallet unlock mechanism or require additional authentication mechanisms (i.e. step-up authentication). See the security section.

For other examples of level of assurance based requirements related to wallet locking see NIST SP 800-63B[6] and the PCTF Digital Wallet Conformance Profile[7].

In proximity use cases, the wallet should be able to present information without requiring the physical device to be unlocked while the holder is advised of what information is being requested and provided a means to consent to sharing it for the specified purpose(s) - see the section on UI/UX for further detail. In this case it is important that the reader is authenticated to prevent any bad actor with a reader nearby extracting data without user consent. This feature protects the users' privacy and enforces the principle of data minimization. Unlocking a digital wallet at the point of presentation may expose sensitive information outside of the context of the data being requested by the verifier, either through theft of the host device or legal authority to inspect/confiscate a host device.

Accessibility and usability must be incorporated into the functional and non-functional requirements of the unlocking mechanism while taking into account associated risks.

[6] https://pages.nist.gov/800-63-3/sp800-63b.html

[7] https://diacc.ca/wp-content/uploads/2023/04/PCTF-Digital-Wallet_Conformance-Profile-Final-Recommendation-V1.0.pdf

Adoption will be impacted If a control mechanism is not usable or accessible leading to the use of less secure methods and/or segments of the population being excluded from using the wallet.

In summary, wallet lock/unlock mechanisms protect the wallet from unauthorised access which includes viewing, adding, updating, sharing and deleting wallet contents based on wallet design requirements whereas relying parties dictate the Identity, Authenticator, and Federation Assurance Levels, as applicable, they require to access their services.

Holder Binding

Digital wallets are applications used to receive, store, and share attributes in a secure, privacy enhancing fashion. To prove that the legitimate, natural person is receiving, in possession of, or sharing these attributes requires a means to bind the wallet and the credentials it manages to the natural person.

In 1995, for example, the International Civil Aviation Organization (ICAO) clearly recognized the desirability of pursuing the use of biometrics in travel documents as the single best way to link the document and its rightful "owner."[8]

In this example, the issuing authority binds the identity attributes to the authorized holder during the issuance process by including biometric data in the cryptographically signed logical data structure. When the holder makes an identity claim, the relying party (verifier) can determine the authenticity and integrity of the identity attributes and, through biometric recognition, determine if the authorized holder is presenting the information during the verification process. This works well for the intended use case: in-person identity verification by government authorities for cross-border travel.

From a safe wallet perspective, holder binding can be split into sub-categories relating to the points in the chain of custody of the wallet and the credentials it contains. It should be noted that chain of custody differs depending on whether the wallet will perform holder authentication during a transaction with a relying party, or whether the relying party will perform holder authentication (e.g. by comparing the portrait image from the authenticated credential to the presenter of the credential).

- Holder binding to the device and wallet.
    - The wallet should have a mechanism to associate, and differentiate, one or more natural persons to the device as part of the wallet provisioning & setup process.
    - Where biometric binding is used, the wallet should have a mechanism to store, and share, associated metadata such as: signature of authority providing the biometric data, live capture by authority indicator, quality

[8] https://www.icao.int/security/mrtd/downloads/technical%20reports/icao_mrtd_history_of_interoperability.pdf

    assessment method & result, presentation attack detection (PAD) method & result, morph attack detection (MAD) method & result
  - The wallet should have a mechanism to store, and share, the associated assurance level of the issuance process (e.g., reflective of in-person, remote supervised, remote; uniqueness determination).
  - The wallet should take any action if previously set up device security (e.g. a fingerprint) is changed (e.g. the addition of a new fingerprint which could come from another person).
  - The wallet may have its own person binding method in addition to the one implemented by the device's operating system.
- Holder binding to their credentials at issuance.
  - The wallet should provide a mechanism whereby the issuer is able to confirm that the person they are issuing the credential to is the correct person.
  - The issuer may be able to insert into the credential (as an attribute or metadata) a confirmation that such a check has been performed, and how it was performed, such that a relying party can confirm what checks the issuer carried out.
- Holder binding to their keys (see Key Management in the Security section).
  - The wallet must have a mechanism to bind the private keys within the wallet that are used for proving possession, for signing, etc, to each holder. For example:
    - Device keys are bound to the device.
    - A holder is bound to the device keys via the device OS.
    - A holder is bound to an identity credential via the biometric contained in the identity credential.
    - The identity credential is bound to the device via the device keys included in the identity credential (and signed by the issuer).
    - A relying party will need a mechanism to determine the level of confidence it can place in each of these bindings.
  - This mechanism should operate within a secure enclave or trusted execution environment.
- Holder binding at the point of presentation.
  - The wallet should have a mechanism to check that the person releasing a presentation ("proof") to a relying party is the same person to whom the credential was issued.
  - The wallet may be able to inform the relying party what mechanism it used to perform such a check and provide evidence of the success of the check.
  - The wallet should support multiple methods for executing holder binding at the point of presentation e.g. PIN entry, biometrics.
  - The wallet should have the ability to configure the holder binding checking it does in response to a trigger in the relying party's proof request, i.e. the relying party can request a high assurance binding check for a high value transaction, or a low assurance check (with less friction) for a low assurance transaction.

Additional information regarding biometrics in holder binding

In each of the Holder binding sub-categories where biometrics are used as part of the binding process, the additional factors described in this section should be considered.

All biometric systems are probabilistic and will produce Type I (false non-match) and Type II (false match) errors which must be factored into the target use case. These error rates are influenced by factors such as quality, which is impacted by factors such as the equipment used to capture the biometric data, the resolution, lighting conditions, pose angles, environment, and demographic differentials.

Relying on a third-party biometric recognition algorithm operating on a personal device to compare a selfie captured in real-time against the selfie captured during registration may be sufficient for some use cases - but not for others. Edge authentication, where the native or a 3rd party biometric sensor and/or matcher is used, is inherently lower assurance than in-person authentication where the relying party's biometric sensor and matcher are used and where the relying party can determine quality and match thresholds.

The EU Digital Identity Wallet legislation[9], for example, calls for Level of Assurance HIGH for User Authentication which necessitates the use of two of three factors where one factor can be inherence. This is where, "the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source;"[10] and "'authoritative source' means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity;"[11]

An 'authoritative source' for high-risk use cases requires biometric data to be captured live by a trusted entity, evaluated to be of sufficient quality for automated recognition, and determined to be unique within the target population to an acceptable False Positive Identification Rate (FPIR) at a specified False Negative Identification Rate (FNIR). This is typically performed by a government agency where, per NIST SP 800-63A and others, the "Expected Outcomes of Identity Proofing" is to "Resolve a claimed identity to a single, unique identity within the context of the population of users the CSP serves."[12] Comparing a physical attribute of a natural person to one encoded on, or in, a government issued credential is NOT identity proofing, it is identity verification.

For identity resolution (aka, deduplication) we are more concerned with the false negatives (the misses) versus the false positives (the erroneous matches) which may be adjudicated manually. This is especially relevant in the Holder Binding to the wallet. For the highest assurance levels, for example, we expect that the authoritative source for biometric data is captured live by a trusted entity and determined to be of sufficient quality for automated recognition.

[9] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_EN.pdf

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502&from=en

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502

[12] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63a.pdf

Regulatory Compliance

For widespread adoption of digital wallets, there must be guardrails in place where both public- and private-sector implementers can turn to understand conformance - and for the public to derive trust.

There is a balance to be struck between the enforcement of legislative rules through technological means versus through a court of law. For example, it may be decided that it is too technically complex to implement some legislation rules into a digital wallet, so the designers may elect to rely on the rule of law as implemented by a court instead. This would mean that the technology does not restrict something from happening in the wallet, and instead, the rules are enforced through heavy fines or prison time for the transgressors.

An example of this in the automobile industry is that enforcement of speed limits in cars is done by the police and the courts, not by the technology in the car (at least not yet).

Some of the identified legislative issues related to wallet-based data exchanges are summarized below:

- Legislations that organizations need to adhere to while processing data. E.g. Article 30 of the GDPR places an obligation on controllers and processors (organizations, issuers/verifiers) to have in place within their organizations a detailed record of activities the organization carries out which use personal data.
- Legislation that ensures the digital rights of the individuals are taken care of. e.g. The GDPR has a chapter on the rights of data subjects (individuals) which includes the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to a decision based solely on automated processing.
- Article 7 (1) of GDPR states that in situations where the processing of data is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data.

As digital wallets become more commonplace, legislation is evolving to catch up. Some examples of privacy-related legislation that applies to digital wallets are:

Regulation	Acronym	Year	Country
General Data Protection Regulation	GDPR	2018	EU
California Consumer Privacy Act	CCPA	2020	US/CA
General Personal Data Protection Law	LGPD	2020	Brazil

Regulation	Acronym	Year	Country
Digital Charter Implementation Act 2022	DCIA	2022	Canada
Digital Personal Data Protection Act	DPDPA	2024	India

This framework cannot and does not intend to provide a list of every piece of legislation in every industry and sector and country that needs to be complied with. Instead, there is a set of questions that a wallet designer needs to answer.

- The digital wallet design must comply with the legislation in place for the use cases envisaged for the digital wallet and the credentials it will contain, and the jurisdictions in which it will be used.

- The wallet should implement technical restrictions to achieve legislation compliance for as much of the applicable legislation as possible. How much logic does the wallet contain to ensure legislation compliance versus relying on legal enforcement?

- The wallet must demonstrate compliance with applicable legislation focused on accessibility.

- The wallet developer must provide evidence of which legislation the wallet complies with, and how that compliance is achieved.

- The wallet must comply with any applicable trust frameworks in the wallet's use case ecosystem and jurisdiction, and the wallet provider should provide evidence of such.

Certification

Certification in the context of digital wallets relates to the formal evaluation of products according to standards such as Common Criteria. It is closely associated with the Legislation Compliance topic since digital wallet regulations in some cases include specific certification requirements.

This framework does not intend to list all applicable certification criteria for all use cases in all jurisdictions. Instead, it provides a list of questions that a wallet designer should be able to answer relating to the certification compliance of their wallet for its intended usage scenarios.

- Compliance with regulations:

    - The wallet complies with national or regional certification requirements. (Example: The eIDAS Revision regulation, where EUDI Wallet certification is mandatory.)
- Components to be certified:
    - Does the digital wallet mobile app have to be certified, and to which certification standard? If so, is the digital wallet certified? (Example: FITCEM certification.)
    - Does the secure element in the mobile device have to be certified, and to which certification standard? If so, is the secure element certified? (Example: Common Criteria or GlobalPlatform certification.)
    - Does the digital wallet backend have to be certified, and to which certification standard? If so, is the digital wallet backend certified? (Example: ISO 27001 audit.)
    - Are there any other components in the digital wallet eco-system to be certified, and to which certification standard? If so, are the other components certified? (Example: HSMs that are Common Criteria or FIPS 140-3 certified.)
- Evidence of certification:
    - The digital wallet provider must supply evidence to the user that its certification is up to date (example: There could be information on the digital wallet's screen that can be tapped on to get more details.)
    - Is there a certification body (in the applicable country) that publishes lists of certified digital wallets?
    - Does the certification body publish certificates or reports about the digital wallet certifications?

User Interface / User Experience

Digital wallets, like other IT, will gain adoption if useful, inexpensive, safe, and easy to use. The User Interface (UI) and User Experience (UX) aspects of digital wallets in particular will drive or diminish adoption. UI refers to the screens, buttons, toggles, icons, and other visual elements that you interact with whereas UX refers to the entire interaction you have with the digital wallet, including how you feel about the interaction.

UI/UX rules

- Intuitive navigation: The digital wallet should be easy to navigate, with clear and concise labels for all functions. Users should be able to quickly and easily find the information and features they need.
- Visual cues: The digital wallet should use visual cues, such as icons and colours, to help users understand what they are doing. For example, a green check mark could be used to indicate that a transaction was successful.
- Threat alerting: The digital wallet should clearly and simply alert the user if it detects that a fraudulent transaction may be in progress, and advise them what to

do next. For example, the wallet should be able to verify that a relying party is legitimate and able to ask for the information they are asking for. It should be able to confirm that an issuer is legitimate and able to issue a credential of a certain type. Conversely, it should let the user know if such checks have been passed successfully and the transaction is safe to proceed.

- Accessibility: Does the wallet comply with industry standards and legal accessibility requirements? Does it offer intelligent features where the wallet can make choices on behalf of the holder? Does it allow the wallet to be accessed via multiple channels (e.g., smartphones, web browsers?
- Security features: The digital wallet should use the latest security features to protect users' data and funds. This could include features such as two-factor authentication, biometric login (aka, unlock), and data encryption. See the Locking/Unlocking section.
- Transparency: The digital wallet should be transparent about its security features and how it protects users' data. This information should be easy to find and understand.
- User feedback: The digital wallet should provide users with feedback on their actions. For example, the digital wallet should notify users when a transaction is successful or when there is a problem.

Resources and References

- OWF Wallet User Experience https://docs.google.com/document/d/1XPgYfd2111NfyUyveIJcXDWjiOdYFPUh/

- UI/UX Design for Digital Wallets: Marrying Security with Intuitive Navigation | by Ethercess | Sep, 2023 | Medium https://medium.com/@ethercess/ui-ux-design-for-digital-wallets-marrying-security-with-intuitive-navigation-61acaa66a2c8 medium.com
- The Role of UX/UI Design in Cryptocurrency Wallet Development | by Naeem Hasan | Oct, 2023 | Medium https://medium.com/@naeemhasan588/the-role-of-ux-ui-design-in-cryptocurrency-wallet-development-3f1fbe97b747 medium.com
- W3C Accessibility Guidelines (WCAG) 3.0 https://www.w3.org/TR/wcag-3.0/
- 7 Best Practices For Enhancing Your Digital Wallet Security https://www.appknox.com/blog/best-practices-for-digital-wallet-security www.appknox.com
- Digital Wallet Design: Enhancing Your User Experience https://qubstudio.com/blog/digital-wallet-design/ qubstudio.com
- How to Improve Mobile UX with Digital Wallets https://cxl.com/blog/digital-wallets/ cxl.com

Counterparties

In the context of digital wallets, a counterparty is a person, organisation or thing to whom a digital wallet is connecting to in order to execute a transaction of some sort. The counterparty could be an issuer of credentials, an online shop requesting age verification, a police officer, or a passport e-gate.

- Counterparty Identity Verification
    - The wallet should inform the user that the counterparty that they are interacting with is who they say they are (see UI/UX section). For example:
        - If the user is being offered a new digital credential by an organization, the user should be able to quickly and easily identify the organization and see that it is legitimate.
        - When the user is being asked to digitally sign a contract, the user should be able to quickly identify the who the requester is and determine that they are legitimate
        - The user should be able to proactively send a verification request to an organization (or another user) to determine that they are legitimate. The wallet may do this for the user automatically.
    - The user should be able to see several levels of detail about the counterparty. For example:
        - Level 1: a visual confirmation (green tick style) that the counterparty has been vouched for by some authority.
        - Level 2: detail about the counterparty's identity, for example company name, registered address, company number.
        - Level 3: detail about the vouching that has taken place e.g. digital signature matches, vouching organization process, Legal Entity Identifier details, legal and regulatory obligations the counterparty may have regarding revealing the shared information.
- Counterparty Action Verification
    - The user should be able to quickly and easily determine that the counterparty is allowed to ask what they are asking, and if it is a reasonable request
        - Some data sharing transactions may be limited by regulation, restricting who is allowed to ask for what. This should be communicated to the user.
        - The digital wallet should be able to automatically reject illegal requests. The digital wallet should support a rules engine, or similar, to determine that a specific request from a specific issuer is illegal in one specific jurisdiction and legal in another.
        - The user should be able to determine that "Gerald's Corner Shop" is not a legitimate issuer of driving licenses, for example. The digital wallet should be able to determine that an issuer is both legitimate AND authorized to issue the type of credential being offered.
        - The digital wallet should be able to alert the user when it detects oversharing.

Audit

Digital wallets should provide the ability for participants in a digital credential ecosystem to know what is happening in that ecosystem. It is tightly linked with the Privacy and Legislation Compliance topics.

Audit requirements and Privacy requirements can and will clash. Care will need to be taken to design a digital wallet that handles both in the best way. The balance between user privacy and regulation is also an important topic, even more so when multiple competing regulations may be involved.

- User Audit.
    - The digital wallet user is able to see all the transactions that they have carried out with their digital wallet.
    - Can these transactions be used as proof of activity e.g. proof of purchase?
    - Can they delete their own transaction list in an unrecoverable way?
- Governance and Operational Audit
    - Ecosystem governance bodies have tools that enable them to audit the correct operation of the ecosystem without harming the privacy of the ecosystem members (issuers, holders, verifiers)?
        - For example, if a relying party is asking for more data than it is allowed to, can the governance body see proof of this to stop it happening again?
- Legal Audit.
    - The digital wallet may need to provide an activity log for one or more actions under legal authority
    - The digital wallet should satisfy local regulatory audit requirements; for example, legal authorities may have the right to examine the content and transaction history of a user's digital wallet as part of a criminal investigation in the same way as they can execute a search warrant to look at the contents of a person's filing cabinet.
    - A legal authority may have the right to access the transaction history of an issuer/verifier and prove that a user interacted with them without looking at the user's digital wallet.

Accountability

Digital wallets are used to access services from Counterparties which may be for nought if the responsible parties cannot ultimately be held accountable. Like most Safe Digital Wallet categories, requirements for accountability can be divided into: a) technical mechanisms (those that can be implemented with hardware, software, and protocols) and, b) governance mechanisms (those that must be implemented by humans following prescribed laws, regulation, policies and/or rules, including via reputation systems).

Checklist for Technical Accountability Mechanisms

These are functions of a digital wallet required to produce what a court of law will consider admissible evidence of the actions of the relevant parties in the case of harm or damage resulting from reliance on the wallet or its contents. Without such evidence, it would be all but impossible to hold specific parties accountable.

- The digital wallet should provide secure storage of cryptographic keys, credentials, and digital assets. If a defense lawyer can create reasonable doubt that the keys, credentials, or assets in a digital wallet were secure, it becomes very difficult to hold the relevant parties accountable since all of them have plausible deniability that they took the harmful action.
- The digital wallet should be able to digitally sign credentials, messages and transactions. Only by applying a digital signature to each action taken by the relevant parties can that action be tied directly to the use of a particular digital wallet in a particular interaction.
- The digital wallet should produce a secure audit log of user and counterparty interactions and transactions? As described in the Audit category (above), only by keeping a history of all the digitally signed transactions will the wallet holder be able to produce evidence of the alleged harmful actions.
- The wallet should provide alerts for unsafe interactions. In addition to compiling evidence, a Safe Wallet can also implement “accountability by design” by designing the wallet software to alert either: a) the user, b) a governing body (such as a consumer protection agency), or c) both if the wallet detects anomalous behavior or a clear policy violation. This “thousand eyes” approach can be a highly effective deterrent for many bad behaviors and dark patterns online.
- The digital wallet should have integrated technical support for a reputation system. This is the necessary technical enablement for user-generated reputation (see #7 below).

Checklist for Governance Accountability Mechanisms

While technical mechanisms can produce evidence or notification of harmful actions, ultimate accountability resides in the ability to take enforcement action when necessary. This can be supported by any combination of the following governance mechanisms.

- The digital wallet should be certified, and if so, under specific certification programs, for specific assurance levels, under a specified trust mark(s). Many governance frameworks will specify certification requirements for digital wallets as well as for issuers and verifiers of specific digital credentials.
- The digital wallet should be conformant with relevant governmental regulations. Many types of digital harms are already covered by existing laws and regulations, including commercial codes, consumer protection laws, and data protection and privacy regulations.
- The digital wallet should be conformant with relevant governance frameworks (aka trust frameworks). Digital wallets, agents, and credentials can be issued, held, and

verified under the policies of a governance framework published by the relevant governing body. Specifications, tools and models for digital governance frameworks are published by the Trust Over IP (ToIP) Foundation; best practices for digital trust frameworks are published by the Open Identity Exchange.

- The digital wallet should be audited for continued conformance. Most certification programs will require either periodic or on-demand audits of the wallet hardware and/or software, as well as audits of issuers and/or verifiers.
- The digital wallet should support a dispute resolution mechanism. While legal enforcement is a court of last resort, many governance frameworks may specify more progressive, efficient, and less expensive dispute resolution mechanisms.
- The digital wallet should be covered by one or more liability frameworks. Another important accountability topic addressed by governance frameworks is liability, i.e., how damages are assessed, allocated, and paid when a party is found to be in violation of a governance framework. Note: because of their ability to automate verifiable transactions, digital wallets may also enable their holders to engage in a unique new form of automated class action. Holders that have suffered a specific harm could give consent via their digital wallets to: a) join the class action lawsuit, and b) automatically send the necessary evidence to the class action litigator. This could be a particularly powerful deterrent to bad actors.
- The digital wallet should support a reputation system. The reputation system should cover the safety features of the wallet itself. Reputation systems are user-generated accountability mechanisms that do not require trusted third parties (other than to design, implement, and prevent gaming of the reputation system).