

Wallet Request

Summary

What should a request to the wallet look like to achieve the purpose of the [Verifier](#) and the privacy of the [Subject](#).

Also known as a Generic Wallet Query Language this proposal has deliberately been formatted as an explainer and not in any existing group's format as it is not clear which standards group is best suited to address the issue. The need for an explainer will exist even after a standard is created.

The primary deliverable is a message that can be created by any verifier independent of media used to transmit the query to the user's device or the format of credentials in the user's possession. The primary objective is to provide the holder of the device with a single screen information display that can be acted on by the user without referencing any other source. That does not mean that the user cannot look at more evidence to make the choice, but that in the large majority of cases the user will not want to look at more evidence. What this means is that the user cannot be presented with just a list of data elements (which might not even fit on the screen) but rather with the reason for the request. The Wallet could determine if it could respond to the request.

As used here a wallet is any app on a holder's portable device that can protect a subject's private data and perform secure creation of holder's intent to be returned to the [Verifier](#).

Context

Today it is possible to use a driver's license issued in California to enter a bar in Thailand. The question arises about how a request from a [Verifier](#) in any jurisdiction can make a request that all digital [Wallets](#) could meaningfully handle to allow existing purposes. The use cases listed below include cases where interoperability of wallets with disparate requirements in diverse identity [Ecosystems](#) are important to the person that selects which wallet to use.

Problems

1. Users will not select [Wallets](#) that cannot get them access to resources that they depend upon. This page focuses on the way to create a request from a verifier such that it can be handled by the wallets that the user is likely to have in their possession.
2. The existing proposal for a database query design language from the Verifier to the Holder's wallet is that it is not possible for a user to make an informed choice and the result is a permanent SQL injection attack as a feature of the design. A more secure, user-friendly design is required.

3. The user is on a multi-user machine (at home or in the public library) and wants to access material that is not acceptable for children. The computer needs to access the user's phone to get proof of age to send to the web site. The phone verifies the user is the owner of the credential.
4. When the request comes to the user's device, the means for routing that request to an appropriate wallet will be a challenge that is not further addressed in the paper. Any solution will require some support from the device's OS.
5. When the request from the [Verifier](#) includes multiple purposes it is not likely that the user can be expected to switch from one wallet to another. Nor is it clear that the user ID will be the same in two different wallets.
6. Many states in the US are issuing [Mobile Driver's License](#) wallets that can only hold their own [State Issued Identifiers](#). Thus using that [Wallet](#) for other purposes of the [Verifier](#) will force the user to select different wallets to gain access to the desired resource. A solution that many users will avoid. Given that the ISO 18013 standards are focused on driver's licenses, it is not likely that state-issued mobile IDs will ever handle commercial credentials.
7. Technologies, including cryptographic methods and communications channels, are changing rapidly. If these changes are not accommodated by users with existing mobile devices, the user will not be able to use them until they upgrade their device.
8. The web deployments need to handle large numbers of requests, potentially with different end-points using different network protocols. Strong context session cookies (including file based session data) need good protection, possibly with encryption.

Use Cases

1. A wallet that holds a California [Mobile Driver's License](#) can be used to enter a bar in a different country with different legal requirements.
2. A shopper at a grocery store wants to give the store their [Loyalty ID](#) in order to take advantage of selective discounts available to loyal customers as they pay for their goods with a payment card also in their wallet.
3. A shopper comes to the cash register with two products (say tobacco and liquor), the request from the cash register, based on the bill of materials is "Do you have ao18 and ao21? The user has two wallets, one can be used (inter alia) for ao18, the other for ao21. Can the chooser pick the right wallet?
4. A sovereign state needs [State Mandated Identification](#) in order to have a consistent [Identifier](#) for any of the several hundred licenses and other uses of that State.
5. A door delivery driver needs to check your age for a wine delivery. You both have wallets on smartphones, but from different OS vendors. It's important to both that the delivery can complete with tap, swipe and a success notice appear on both phones.
6. A user going into a gym with a membership may need to show three different cards which they can now hold in one hand as they go past reception. Digital wallets need the same multi-credential ease of access.

7. A holder might have authority to hold credentials for multiple subjects, like children. Some transactions, like proof of presence, must be able to distinguish between the subject and holder.
8. Controlled over-the-counter medications may require a name and residence locality for quantity tracking.
9. Supermarket cases can be extremely complicated. Generally a transaction starts with a membership card so that the price can be accurately shown on the transaction display device. If the transaction is at a special booth (like an in-store coffee shop) might require more than one membership card or a health insurance card. Depending on the merchandise scanned additional ID (like ao.18) might be needed to allow the transaction to complete. At payment different payment cards might be appropriate like health insurance, food assistance or other types of alternate payors. For the case of partial payments the holder may need to provide a second payment method to complete the purchase. Supporting this case without confusing the holder will be a major undertaking.

Purpose

For the purposes of the request, “purpose” is related to the Verifier’s legitimate needs. Getting a better realization of purpose in the request is necessary before a request can be shown to be compliant.

When is data processing allowed? From Data Protection under the GDPR

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

EU data protection rules mean you should process data in a fair and lawful manner, **for a specified and legitimate purpose** and **only process the data necessary to fulfill this purpose**. You must ensure that you fulfill one of the following conditions to process the personal data; you:

- have been given the consent of the individual concerned
- need the personal data to fulfill a contractual obligation with the individual
- need the personal data to satisfy a legal obligation
- need the personal data to protect the vital interests of the individual
- process personal data to carry out the task in the interest of the public
- are acting in your company's legitimate interests, as long as the fundamental rights and freedoms of the individual whose data are processed are not seriously impacted. If the person's rights override your company's interests, then you cannot process the personal data.

Solutions

This page describes two ways to handle requests from wallets that need to serve multiple purposes in a single request to the wallet. While it is possible that a wallet could handle both types of request, interoperability would be improved if only one of these methods were selected.

1. Allow the request to contain both optional and required claims and list multiple purposes as advisory and not directly connected to the list of claims required.
2. Allow the request to contain multiple purposes and let the holder make a choice on which purpose to consent. In many cases the purpose should be sufficient to determine the claims provided by the wallet. This has also been called the collection of transaction sets, where each transaction was related to one purpose. It is also possible for each purpose to list the specific data elements (claims) that are needed, but the long term goal would be for the purposes to be sufficient for that purpose. Each purpose could be required or optional, but any data element listed in the purpose would be required.

Note that the field "scope" in OAuth or OIDC could include the purpose.

Changes needed from the Device or Browser

There is currently a proposal to address [Digital Credentials](#) in the W3C WICG. This particular proposal is focused on getting an app in the browser to select the right wallet. What is still missing is a means to instantiate this "metawallet" that could expose any choice to the user. The best user experience is to just select the wallet and let the wallet ask the user to express their intent. The one corner case is where the user has two credentials which address the query from the Verifier. Perhaps users could be given the ability to configure this "metawallet" to make the choice for them.

Contents of Query

These are proposed data for the query from the Verifier to the wallet.

The security for this message has yet to be formalized. It could be the inclusion of federation Metadata or a cert from a trust registry or as part of a signing key.

Name	Req Status	Examples	Details
Name of Verifier	Required	Joe's bar and Grill	This is the dba name that the user should recognize
Data Processor	Optional	Stripe	The legal name of the entity retaining user data
Contact	If data retained	Remove data	URL or mailto: link
T&C	Discouraged	25 pages of legalese	terms for legal purpose
Authentication	Option	PoP IAL	level of security
DateTime	?	Not trackable	Limit to YY:MM:DD:HH of notice
Reference	Option	Trackable	nonce
Jurisdiction	Option	EU US-CA FHIR	legal or trust zone or federation
Purpose and scope	structures	buy liquor	required yes/no
residence	if state require		each field is required

None of these ideas or names originated with the paper. Some of the sources include:

- [ANCR-TPI-Conformity Specification v0.9.pdf](#) Advanced Notice and Consent Receipt - Transparency Privacy Indicator dated 2023-07 (To see the whole doc you need to keep clicking on "show more data")

Purpose Structure

There are a large number of reasons why a Verifier might ask the user for verified claims of one sort or another. In some cases the purpose can easily determine the data field to supply. For example the requirement for a minimum age for COPPA is 13. In that case the purpose could be that the user has passed their 13th birthday which could be coded as "ao.13".

The purpose will be coded as rurl?code. Where rurl is a URL in reversed order and code is any ASCII string the registry desires. The rurl "0?" (or the absence of an rurl) means the purpose code table described below. The optional data element (claim) list would be a json string similar to that proposed in other standards organizations. For example {eu.purpose?code) could be a table created by the eu and put at the location <https://purpose.eu>.

Purpose Registries

The purposes that the Verifier can select can be simple, in which case a list from this document could be used. In others they are part of a federation that determine which user attributes are needed to meet a given purpose. For example in medicine if the purpose is "create a prescription" attributes like allergies must be provided to avoid selection of a medicine that could cause harm.

The goal is for a local decision (no web lookup) if possible. The following are a few of the common purposes that could be included in a standard as the base set of purposes agreed by all:

code	Name	Example	Details
ao.xx	adult	ao.13	the minimum age to avoid regulation like COPPA rules
sub	subject name	jose palme sierra	Composed of surname: "Palme Sierra" and givenname "Jose"
member	loyalty	999-999-9999	These cards are typically designed to allow the holder to get either discounts or extra services, phone # is common
types	category	grocery	This information on the purchase is needed if the wallet is to make a choice as to which payment types are acceptable
residence	location	King	The residence response could vary widely and perhaps some finer level is required. A query as to your state residence could be responded with just a two letter code, a zip code or a yes/no.
vax	vax status	yes/no	The local requirements for vaccination could change daily during a pandemic. The question about where verification would actually be performed is open at this point.

References

- A request to create a work item for this was sent to OpenID
<https://bitbucket.org/openid/connect/issues/2121/enable-a-device-to-direct-requests-from>