Inclusive Purpose Consent Query (PCQ:)

Version 13 KI-RIUP-WG draft - Date 2025-02-18

Contributors

Justin Byrd, Salvatore D'Agostino, Jorge Flores, Jim Kragh, Tom Sullivan, Noreen Whysel, Tom Jones

Abstract

The Inclusive Purpose Consent Query is designed for a Verifier to send sufficient information to a smartphone to enable the holder to fully and quickly understand the query. The message may suffice for common, simple queries to acquire all the information a verifier requires. At the very least, it will establish a connection to a user agent (like a digital wallet) which can continue the query process. This document is not intended to be a complete formal specification but should be treated as an explainer for understanding the requirements for a broad range of inclusive use cases.

An inclusive query can be handled by all people who are entitled to access a service or other resource. To become inclusive a query must be able to be processed even when the holder or the subject is:

1. Not able to communicate in the local or preferred language,
2. Aware but not capable of handling the requirements of digital devices,
3. Unable to give informed consent on their own behalf,
4. In an emergency location where network access is not available.

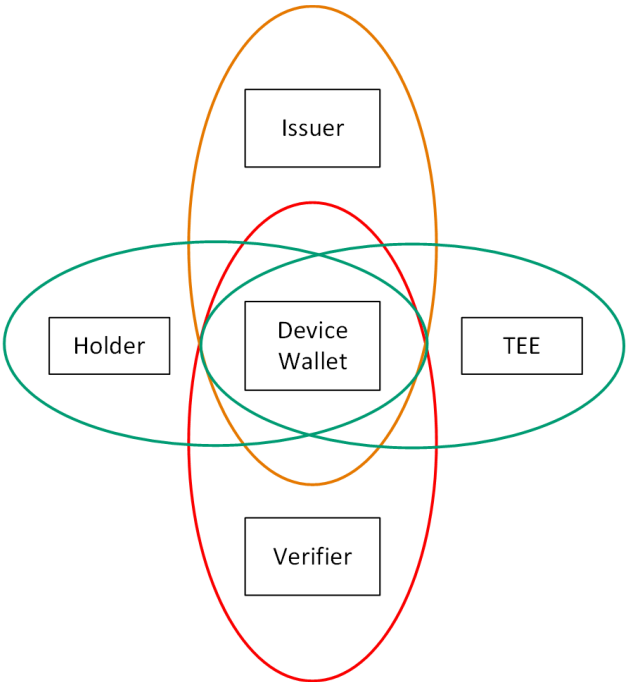
Goals

This is the verifier subset of the identifier ecosystem's goals stated elsewhere. This specifically addresses the needs of a human Holder of a wallet to get the information that's needed to make an informed choice to share data. This document addresses only the digital interaction and not local signage which would also need to be accessible to the wallet holder. (Kantara PEMC 2024)

1. The only use cases addressed here are where the Verifier initiates the Query to a device in the holder's possession. Either the device or a wallet app on the device will be able to accept the query and respond appropriately.
2. Functional for all subjects with digital credentials that are needed for their day-to-day transactions, with no exceptions.

3. If the subject needs a delegate to get necessary access, the wallet and verifier will accommodate multiple subjects or holders for a single device.
4. Works for first responders like medical technicians or disaster recovery operations where internet connectivity is not available.
5. Audit and fraud detection is built into the basic functionality.
6. A Query can be generated by a simple device in a small shop with all of the information required by the shop to complete the transaction. This should include payment as well as age verification, for example. An internet connection is not required to complete the transaction for any normal use case.
7. This query will help small verifiers to show compliance with privacy standards like the Kantara Privacy Enhanced Mobile Credentials (PEMC 2024).
8. Show use cases where a delegate is needed to release a subject's data where the subject is not able to make the response on their own.

Problem to be Solved



The user agent (which will be called the Wallet below) runs on a mobile device that enables a Holder to acquire credentials from Issuers and protect them with a Trusted Execution Environment (TEE) that may, or may not, be an integral part of the Device that hosts the Wallet. The diagram shows the Privacy Boundaries that need to be defined, centered around the Wallet, to protect the private data of the subject. The Holder needs to be in control whenever data moves across boundaries. The Wallet, running on the user device is within all four boundaries and so should only allow data to cross any boundary with the holder's consent. That means that any personal data transfer will be under the direct control of the holder's wallet. The data that stays within the Wallet (the green boundaries) is under the control of the Holder. Credential data is sourced from the Issuer and acquired by the Wallet (the orange boundary) when acceptable by the holder where it is protected using the Trusted Execution Environment (TEE). Any data sent out to the Verifier (the red boundary) must be approved by the Holder before it leaves the Wallet.

The Wallet knows nothing about the Verifier before the query is received. So the query must provide trust context to the wallet so that it can display a trust assurance that the

user can understand. Presumably, the trust context would include a signature and certificate of some sort together with a Trustmark appropriate to the trust context. It is also possible that some trust can be inferred from the physical context of the Verifier.

When the user indicates consent to process the request then the first step of trust establishment is completed. In the simplest case, the presentation response from the holder to the verifier will allow the completion of trust establishment. If the user does not consent to share information with the verifier, then trust is not established and other solutions may be offered to the user by the device.

If a wallet sends a response and the verifier rejects that presentation response, the verifier knows that the device is listening and may be able to continue the interchange by sending information to the holder's wallet to allow a different response; for example, if the holder has a different credential that might work.

The query is sent to the holder's device which selects the appropriate wallet to process the request. If the device cannot find a wallet, it may be able to help the holder locate an appropriate solution. For example, applications in a central app store that can process the PCQ: query could be recommended to the user. The communications can be as simple as a query/response or could evolve into a long-term trust relationship.

Context

There exist efforts to standardize the way that applications running on user devices can communicate. For example, the W3C WICG (Cappalli 2024) is working on a way for the browser to route a request to an appropriate wallet application to process the query string. What is missing is the means for a verifier to create a query request that can be captured by Near-Field Communication (NFC) or Bluetooth Low Energy (BLE) and route that request to an appropriate wallet application including any application that needs to be started to accept the request. This document addresses that requirement as well as the broader requirement to give the user the information needed to make an informed consent decision. It is suggested that device operating systems use this technique to direct requests coming into those (and similar) radio channels.

This document is dependent on the Kantara Report on Digital Identifier Inclusion (Kantara RIUP 2024). The term ”Holder" is the controller of the Wallet. The subject of a credential in the Wallet might be the holder or some natural person who has delegated responsibility to the holder and wallet. To be inclusive in all of the times and places where an existing hardcopy document has been used the following list of use cases should be addressed.

1. The holder is trying to get access to transportation for themselves and a dependent child.
2. The holder is trying to get assistance in the aftermath of a disaster where the internet is not available when the assistance is needed.
3. An officer of the government on foot is asking for identification for permission to access some location, or even for proof of right to be in a particular location. How can the holder know that this officer has a right to request this proof.
4. A migrant is asking for access to an administrative law judge to prove that they are eligible for asylum.
5. A non-ambulatory resident of a nursing home needs to grant permission for some procedure to be performed.
6. A non-citizen parent is registering a dependent child for school or health care.

This list is aspirational and not all of them might be addressed in the earliest implementations but must be considered in any approved architecture for wallets.

Complexities

There are situations where multiple purposes can be requested resulting in multiple credentials in very different formats which might be processed in different code bodies in the verifier.

Encryption of messages has been proposed to improve security and privacy. This means that the message may need to be decrypted before it can be determined if the message is to be addressed by one or more different functions that are not part of the receiving function. Encryption of a query could lead to denial of service attacks against the receiver of the message because of the extra processing load on the user's device.

User Experience

Success for this proposal will be an ecosystem for verifiers and subjects of credentials that is an improvement over what can be achieved today with a leather wallet containing cards issued with a variety of credentials that the holder needs in their normal activity of the day. The success of digital representations of credentials will only be possible if the holders and verifiers are satisfied with the results. Good experiences are already evident at many airports in the US. The major change needed is the presence of readers (like a kiosk or transaction terminal) at small merchants, door delivery personnel, and other locations that holders experience multiple times a day. Another verifier that specifically addresses inclusion would be a safety-net service that needs to provide continuity of care or deduplication of services. In every case, the holder must have all the information needed to make an informed decision to grant access to the requested subject data.

Delegate Use Cases

Create delegated digital credential content such that the holder may access any resource that the subject wishes to delegate, either short-term or longer-term.

To be inclusive any solution must be able to accommodate any natural person that is not capable of using common mobile digital user devices, like smartphones.

- Comatose, severely impaired, or young child (Cognitively unable to Consent)
- Language issues (Communications limitations to give informed consent)
- Elderly parent that needs assistance (has become dependent but can delegate consent)
- Other emergency use cases like natural disasters such as Hurricane Helene that struck North Carolina unexpectedly in December 2024. .

Purpose

The purpose is designed to meet the desires of the verifier which includes compliance with local privacy requirements. The following wording is taken from the EU GDPR but should satisfy most jurisdictions. The EU website describes when data processing is allowed: "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 the data controller (aka verifier) should process data fairly and lawfully, for a "**specified and legitimate purpose"** and only process "**the data necessary to fulfill this purpose".**

The other source of compliance information comes from the (ACM 2018) Code of Ethics and Professional Conduct section 1.6 which requires "Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined, enforced, and communicated to data subjects. Personal information gathered for a specific purpose should not be used for other purposes without the person's consent. Merged data collections can compromise privacy features present in the original collections."

Name Value Pairs of data

Name	Req	Value	Notes
ver:nam	R	Name of the verifier	Note that this will be in the localization of the verifier – if more than one alphabet is used, it should all be in one string (trademark) - an array of string
ver:net	O	net ID of the verifier	The network address of the data processor URI, DOI, DID, etc.
ver:pro	O	Name of processor	for example square province POS device
ver:vid	O	ID of person	an employee or badge number and may include if gov't official or authority
rec	D	Record number	Required if data will be retained
ver:ctd	D	Contact of processor	Required if data will be retained
nonce	O	Establish session	eg EPOCH time
date	O	Date request created	EPOCH time
jur	R	Jurisdiction	EU US.CA of the verifier
trust	O	What framework?	of the verifier eg eIDAS, HIPAA, SEC
pur:pcd	1	Purpose code	See table below
pur:typ	D	URI of purpose	Required if code = X
pur:exp	O	Epoch date of retention	If more than 24 hours after the current date for any purpose, the rec and ctd are required.
pur:dat	O	Data elements	Any specific data elements required by the verifier. The goal is that this field is empty.
ath	O	Authentication factors	Any additional requirement for the wallet to provide, such as proof of presence or liveness
acc	O	Accepted protocols	Let the verifier give the device and wallet hints about what protocols will be acceptable to the verifier.
trans	R	Transparency	A formal statement of the Verifier's terms and conditions.

Requirements are: Required, Optional, and Dependent on other contents of the data or at least one entry is required.

Authentication may be indicated in the "ath" code if performed by the wallet, or by a Biometric purpose so that the authentication can be performed by the verifier.

The expiration date (exp) is the last time the data may be retained. Note that subsequent accesses may result in a new consent from the user for the same data that the user has provided previously. The consent applies to the purpose so that a biometric

authentication factor may have a short retention period (less than one day) in which case that data is not considered to be retained by the verifier.

Purpose Code	Name	Notes
A	Age restriction for purchase or access	Followed by one or more integers, 13 18 21
D	Driver's License	Data needed for a license to drive
F	Fishing License	Data to show fishing or hunting license
E	Emergency	The verifier is a licensed first responder
X	The purpose is a URL	This is not for a point-to-point exchange
V	Visa or similar	Proof of permission to be in a country
B	Biometric data	An authentication factor
W	Right to work	Maybe from many different creds.
P	Payment required	May be followed by a currency code
L	Asylum request	From an application for any credential

An example of an overall JWS definition that could follow this structure (before it is minified and compressed):

```
PCQ:{
 "ver": {
    "nam": "<<Verifier name>>",
    "url": "<<Verifier URL>>",
    "pro": "<<Name of processor>>",
    "vid": "<<ID of person>>",
    "ctc": "<<Contact https: or mailto:>>"
  };
 "rec": "<<record number>>",
 "jur": "<<jurisdiction or trust zone>>",
 "ath": "<<other requirements for authentication of user>>",
 "pur": [
   "pcd": "X",
   "typ":
     "https://smarthealth.cards#health-card",
   "exp": 1591037940,
  ]
}
```

Message Flows and Experience

The query goes from the verifier to the holder's device which determines which wallet application (wallet) in the holder's device gets the request. Once that user wallet has the query it creates a display for the holder's consent. After the holder's consent (which might only be for some of the purposes proposed by the verifier, the wallet builds a

response to the verifier. The holder experience from the device or browser and the transition to the wallet will be key in user acceptance of this flow.

Verifier Authentication

It is desirable for the wallet to authenticate the verifier so that the user is confident about who their counterparty is before sharing their data. This is one way to prevent fraudulent data requests. It is also possible for authentication of the verifier to support non-reputability, allowing wallets to present evidence that they were requested from a data set from a particular verifier. This is useful for reporting abuse of the system and inappropriate request patterns to governing authorities. However, methods to authenticate the verifier will vary significantly based on the protocols used for data sharing. It is recommended that the wallet combines the data from the `acc` field (accepted protocols) along with other request data to properly authenticate the verifier if supported by the protocols. Protocol authors are encouraged to create extensions to their protocols or specific guidelines on the interoperability of this specification and mappings to their own for correct authentication of verifiers (for example, see 9.2.4 mDL Reader authentication in ISO/IEC 18013-5:2020). Implementers of relying party software making the requests should ensure that the data fields in the request are adequately populated to allow supporting wallets to perform the desired authentication of the verifier.

Consent

The response from the wallet will come only when the holder consents to the query message. The following are the considerations by the wallet in making that decision as to what data may be returned to the verifier. Biometric data is one element that needs attention as the biometric tests may be performed by the wallet but then the wallet must provide attestation as to its provenance. It is unclear whether privacy is improved by performing the biometric test in the wallet and thus requiring attestation about the wallet which could result in tracking data about the holder.

The user experience by which consent is indicated on the device is under the control of the device and may include previous holder settings or be delegated to a wallet user experience based on the request. Consent is required to allow any information to be sent from the Wallet to the Verifier. One possible response is for the device to establish a connection between one of the holder’s wallets and the verifier based on the contents of the query.

Response to Verifier

This list includes all of the data sent to the verifier as a consent to communicate, possibly with data for similar cases.

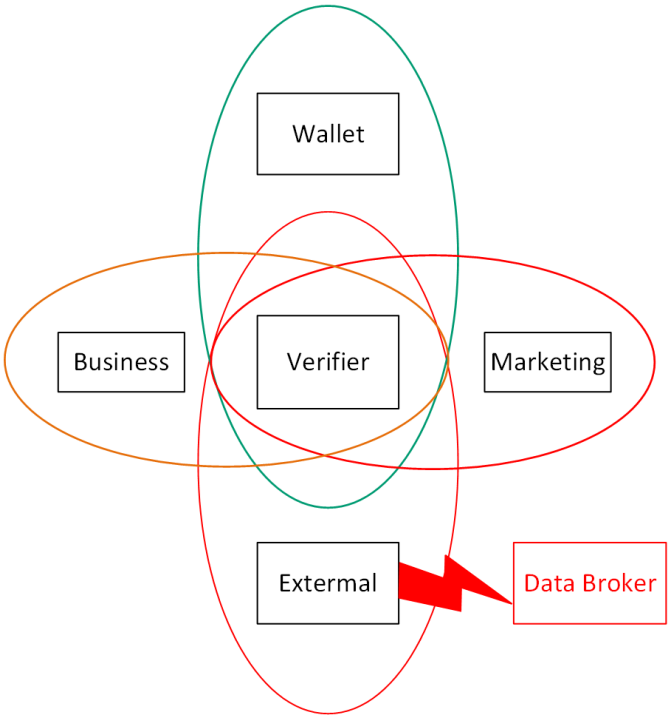
Device identifiers that might be included in a wallet attestation:

- DeviceUniqueId – trackable undesirable
- Shared device indicator (holder not same as subject)
- Device binding - problematic unless it can be tokenized
- UserAgent / Wallet loadable package ID SBOM, etc
- Wallet app instance ID - trackable unless tokenized
- Model
- Manufacturer
- Device Type
- AppID (from the app store with version #) - not inherently traceable
- Bundle ID (apple & google)
- Build Number
- etc

Name	Req	Value	Notes
dev:ref	R	Name of the provider	Typically, the o/s id and version
dev:net	O	net ID of the wallet	The way to access the user wallet app, if missing the device could not find an app that could respond to the request
rec	D	Record number	If provided by the Verifier
ctd	D	Contact of processor	If provided by the Verifier
Jur	O	Jurisdiction or trust zone	EU US.CA HL7
res:pcd	1	Purpose code	See table
res:typ	D	URI of purpose	Required if code = X
res:exp	O	Epoch date of retention	If more than 24 hours after the current date for any purpose this is considered consent to allow retention for the time specified
res:dat	O	Data elements	Any specific data elements required by the verifier
ath	O	Authentication factors	Response from request for AuthN
acc	O	Accepted protocols	This indicates the credential type responding. (could this be res:acc)
org	R	Origination data	Epoch date response created

Verifier Processing of Holder Response

This section is not part of this recommendation but only offers guidance on how the subject data is processed once it is received by the Verifier for the purposes expressed in the query. It is insufficient to just provide the subject's private information to the verifier, but it must be associated with the purpose which is described as the context by (Helen Nissenbaum, 2009). This means that within the Verifier there must be boundaries which data must not cross. First, the data is passed from the Wallet to the Verifier,where there can be some data which is used only for the business purpose that the user wants to accomplish, and other data which can be used for marketing or for validation by external partners of the Verifier. Included in external partners are the Issuer of the credential as well as other assurance checks like credit bureaus. As indicated by the path from the external partners, control of the data is not limited to the Verifier as so could be used for purposes the user never anticipated. As shown in the figure to the right, there are data boundaries that the verifier needs to respect with the data in their possession.



Once in the Verifier's possession, it is still bound by the purpose and duration information provided to the holder in the query. The binding provided in the response message will apply to the data in possession of the verifier and in possession of any third-party service used by the verifier. The binding is shown as a single box labeled "Verifier."

The purpose may additionally allow for the passing of the subject data to other entities to fulfill the purpose; shown here as the orange boundary. The other security boundaries (shown here in red) are more problematic.

When Verifiers want to be able to send future marketing information based on the interest shown by sharing information which includes email or phone number with the Verifier in the first place. Any such request should require an option to include (opt-in) such permission, rather than then need for the user to opt-out of such sharing.

Even more problematic is the sharing of the subject's information with external partners, especially when such sharing is required to establish trust between the subject and the verifier. It is this step that often results in the subject's information leaking out to any site that can sell this information. Such leakage can be deliberate, or accidental. When inadvertent (accidental) sharing occurs it is incumbent on the verifier to let the subject (or delegate) know when this occurs. This section is based on content from the (Kantara PEMC 2024) "Recommendations for Privacy Enhancing Mobile Credentials" and the –Kantara ANCR–

References

ACM 2018 Code of Ethics and Professional Conduct
https://www.acm.org/code-of-ethics

Tim Cappalli 2024-03-01 "Web Platform and App Platform Layering / Interactions" https://github.com/WICG/digital-identities/blob/main/resources/DigitalCredentialsAPI-Layering-v20240301.pdf This addresses a similar problem from the point of view of the browser that is connected to the internet.

Ryan Galluzo +3 2024-10-07 "NIST IR 8480 (Initial Public Draft) Attribute Validation Services for Identity Management: Architecture, Security, Privacy, and Operational Considerations" https://csrc.nist.gov/pubs/ir/8480/ipd

Kantara PEMC 2024-10-10 "REVIEW NOTICE FOR PUBLIC COMMENTS AND IPR REVIEW: PEMC Recommendations for Privacy Enhancing Mobile Credentials v1" https://kantara.atlassian.net/wiki/spaces/GI/pages/683507722/PICPR20241010

Kantara RIUP 2024-09-23 "Kantara report on Digital Identifier Inclusion" https://kantarainitiative.org/download/riup-digital-identifier-inclusion-report/

Helen Nissenbaum, 2009 Privacy in context: Technology, policy, and the integrity of social life. Stanford, Calif.: Stanford Law Books **ISBN** 978-0804752374