**Version:** 1.0 draft 13

**Document Date:** 2025-02-18

**Editors:**

**Contributors:** Justin Byrd,  Salvatore D’Agostino, Jorge Flores, Jim Kragh, Tom Sullivan, Noreen Whysel, Tom  Jones

**Produced by:**

**Status:**

This document is a Group-Editors' Draft produced by the . See the Kantara Initiative Operating Procedures {op href} for more information.

**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.

**IPR Option:**

‑Non‑Assertion Covenant

**Suggested Citation:**

*Inclusive Purpose Consent Query 1.0 draft 13.* Kantara Initiative . . Kantara Initiative . HREF

NOTICE



‑

Copyright: The content of this document is copyright of Kantara Initiative, Inc.  
© 2024 Kantara Initiative, Inc.

Table of Contents

[1. Goals 4](#_Toc191158809)

[2. Problem to be Solved 5](#_Toc191158810)

[3. Context 6](#_Toc191158811)

[3.1. Complexities 6](#_Toc191158815)

[3.2. User Experience 7](#_Toc191158816)

[3.3. Delegate Use Cases 7](#_Toc191158817)

[4. Contents 9](#_Toc191158818)

[4.1. Purpose 9](#_Toc191158820)

# 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 de-duplication 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.

## 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.

# Contents



## 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.”