Receipt Demo v2

On the December 6, 2018 CIS WG call, we came to a rough consensus about what scenario we would like to show in the next version of the demo: **The Kantara Initiative Privacy Control Panel system.**

EIC and Identiverse have accepted our proposal to show the demo. Will be submitting a proposal to ID North and MyData.

System Concept

The following is a very early draft description of the system we will demonstrate at EIC 2019 and other events.

The main purposes of the Kantara Initiative Privacy Control Panel (Kantara PCP) system are a) to allow people to see, organize, find details via a 'data processing receipt' construct about the conditions under which they agreed to provide information for data processing; and b) to give them tools to investigate the data processing receipts they might have received or modify the permissions they granted when they initially shared the data for processing.

In the Kantara vision, whenever an individual is asked for their personal data, or whenever their personal data is acquired, a 'data processing receipt' is created by the data controller. The receipt includes details about the conditions under which the data was obtained: the privacy notices provided; the lawful basis and purposes for collecting and processing data; the terms of the agreement and other metadata related to the interaction.

These data processing receipts could be offered by the data controller's system to the individual for storage in their personal Privacy Control Panel application.

Once the data processing receipts are in the personal PCP, the person can organize them and inspect them to ensure they are valid, current and actually represent what happened.

The PCP gives the person tools to take action with the receipts including view, validity check, request the data, revoke consent, change permissions, or erase the data. In other words to exercise their data subject rights.

On the consent management platform and data controller system side, standard data processing receipt APIs could be offered. The PCP utilizes these APIs.

The Kantara Members in the Consent & Information Sharing WG can participate in the demo by showing their product features that provide the different functions needed for the PCP demonstration, for example: the PCP dashboard, the data controller functionality to generate receipts, API platform provider, the 'app' used by the person, receipt viewer, receipt language translator, and so on.

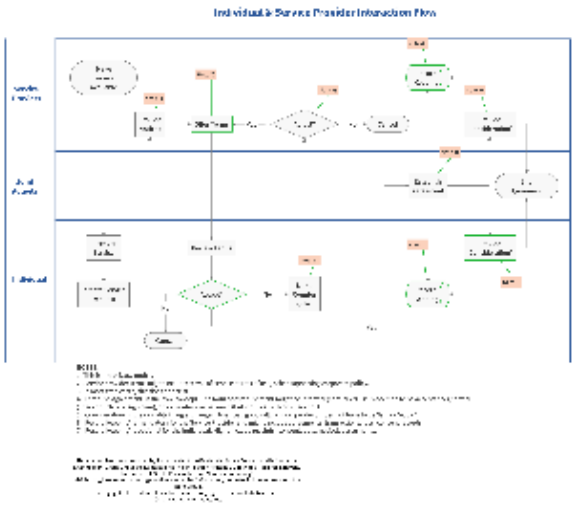
The concept is that the products could, with very minor enhancements, be a component of the overall Kantara PCP system. We will showcase a future vision of the data processing ecosystem where the individual has more insight and control over their data.

The detailed demo functionality will also allow the CIS WG to identify needed changes to the core specification and additional specifications in the data processing receipt family.

Related Meeting Minutes

DRAFT 2018-11-15 Meeting notes (CR)

Baseline 'Agreement' Flow



PCP Roles Table

To help decide which products will perform parts of the demo (Table copied from 2019-02-14 Meeting notes (CR) DRAFT on February 20 2019):

Role	Functionality	Product
Data controller application (A)	The application that the person interacts with - it orchestrates the Notice display, acceptance of terms, creation of receipt and delivery of the intended service Orchestrates the person's "Consent Journey" Option 1: Web application Option 2: Mobile app ** For example, In Demo v1 it was the Bookstore app	Airside? Ubisecure digi.me 'SocialSafe' Sphere OpenConsent
Receipt generator (API?) (B)	This role might be functionality within another role. It takes inputs from the data controller application and returns a conformant receipt in JSON or JWT format Option 1: Functionality within the (A) Data Controller Application Option 2: Functionality within the receipt management platform Option 3: Standalone receipt generator	digi.me Ubisecure Sphere OpenConsent
Receipt storage facility (C)	This is the storage place for the receipts. It could be as simple as the downloads folder or a personal data store or browser local storage or other API The storage facility MUST be readable by the PCP Dashboard role Option 1: Functionality comes from the Operating System Option 2: Functionality included in the (A) Data Controller Application Option 3: Functionality accessible via the receipt management platform Option 4: Functionality in a separate application that does personal data management Option 5: Function accessible via Browser APIs (e.g. local browser storage) ** For example, "wallet" concept; Downloads folder; browser storage; etc	digi.me (consent manager) Sphere Dativa

PCP Dashboard and Control Panel Function (D)	Dashboard - Reads the receipt storage facility and displays the person's receipts in some meaningful and usable way Control Panel - The part where a person clicks on a button against a receipt that causes an action to start Option 1: Functionality exists in a product today Option 2: New product required Option 3: Functionality exists via a receipt management platform and can be called	Sphere digi.me (Consent Access screen)
Receipt management platform (E)	Communication substrate - e.g. one possible function: when user clicks on button to exercise a data subject right, this calls the platform which sends instructions to the data controller to take action	digi.me Sphere
Receipt Viewer app (F)	This displays a receipt - takes JSON or JWT as input and displays in human-friendly way - to allow the presenter to walk through the contents of a receipt with the audience Option 1: Functionality exists in (D) Dashboard/control panel Option 2: Standalone application or web site Option3: Functionality exists in (E) Receipt management platform	Airside? OpenConsent Sphere
Data controller registration	(ACH: What does this do?)	Maybe OpenConsent? digi.me
Receipt language translator	RANDOM IDEA - Display the receipt in a different language e.g. French	