During the past two bi-monthly sessions the FIRE and HIA the WG’s, members provided their input in forming a new Kantara Charter. There was agreement on the internet’s explosive enterprise of connected things, i.e. smartphones and sensors, and the impact on privacy, security and need for digital identities. But that did not answer the following questions when engaging the internet:

* What does an individual, granularly, want to feel? Trust!
* We have experienced face-to-face trust; how do you know

who I claim to be? What assurance do you have it’s me?

* What is a trusted identity? What is a Framework?
* Yes, I have a smartphone, you say it does what? How

can I trust that ‘device’ with my confidential info or private data?

* How does a user gain a ‘comfort level of trust’ when online?

Work Group members collectively underscored the need to develop a consumer centric strategy for individual online users so they could gain insight on what a Trusted Identity is and the value it may be online. We would need to outline and define basic steps on how one might develop online trust, then test examples with feedback for different age groups, cultures, markets and industries. As noted in earlier discussions, a consumer’s authenticated trusted identity must be portable and adaptable to sectors/industries of their choosing. Since healthcare is highly regulated and integrated with multiple industries, and in need of a trusted identity solution that is our initial recommendation which we believe compliments the Kantara mission.

If a trusted identity solutions is adopted by the Government, the savings could be beneficial for Government so incentives should be a consideration when supported by an audit trail? In healthcare there is a very positive upside for payers when patients are compliant in taking meds and following care plans, especially those with chronic conditions, recognizing that healthcare expenses consumed 19.7% of our gross national expenditures, ($4.1 trillion; $12,530 per person) in 2020. Of that, 47% of those dollars were spent on about 80% of the population\* in 2020 (a disproportionate share) who have at least one chronic disease; many who fall short in managing such; not accountable! There are positive up-side benefits for online users to having an authenticated, Trusted Identity. (Data source: HHS-\*tax supported medical care; intent-to promote greater consumer involvement in managing their care.)

Where to start?

During the 2020, Covid-19 crises, the public health population across the country was seriously impacted due to lack of government records relating to personal poverty, food security, housing stability, living conditions, access to quality health and transportation. Yes, health service and food stamps were provided but data was siloed and not always accurate. Last year the Healthy People 2030 Trusted Source campaign was launched. The Government now recognizes conditions in the environments where people are born, live, learn, work, play, worship, and age significantly influence their health. The 2030 goal is to have valid, reliable, nationally representative identified data.

The majority of individuals in this healthcare sector population have smart phones with social identities and they will be future candidates with the support of local governments and local social service entities. With the Executive Order for Zero Trust by late 2024 and NIST, responding to the Executive Order with the draft Recommendations on Criteria for Cybersecurity Labeling for Consumer Software and Internet of Things-Products, is setting the stage for a ‘Trusted Identity’ process at some Assurance Level at State and local government levels. The individual, being an online user, most likely will seek some value content support from a trusted, not-for-profit source like Kantara.

Future subject material for discussion:

* Relying Parties
* Access Controls
* Identity Assurance Level
* Authenticator Assurance Level
* Federated Infrastructure and Identities