**1) WG NAME (and any acronym or abbreviation of the name):**

***Resilient Identifiers for Underserved Populations Work Group* (RIUP WG)**

**(2) PURPOSE**:

The purpose of the Work Group is to support vulnerable and underserved populations in America. At a high level, these populations include those with physical and cognitive disabilities, or who are homeless, impoverished, senior citizens, immigrants, incarcerated, institutionalized and otherwise underserved minority groups that need digital credentials to access online resources; particularly, online healthcare and financial resources. Without an easily reusable identifier, it is nearly impossible for these individuals to gain secure access to the resources and services that may be available to them.

We will work, in collaboration with other private sector and public agencies towards establishing identifiers and access management (IAM) solutions that respect privacy, promote efficiency, limit redundancy, reduce barriers to use/adoption, increase interoperability, improve security, enhance safety and trust, eliminate identification errors, support resiliency, and achieve greater empowerment across the entire spectrum of online transactions. The RIUP WG will identify, coordinate, innovate and harmonize with ongoing and emerging identity initiatives, standards, and technologies, and communicate our findings to all relevant stakeholders, both in the US and, selectively, with other countries, under the leadership of the Kantara Initiative.

**(3) A SCOPE –** Guidelines for Cultivating a User-Centric Trust and Promoting Adoption within Underserved Communities

To advance a user-friendly, authenticated digital identity platform that will elevate online trust for vulnerable and underserved persons, including both adults and children, and accelerate secure, convenient access, accessibility and accountability, enhanced user privacy of these populations and their delegated caregivers must be protected. The goal is not to advance more challenges and bottlenecks to exploit but to deliver user-friendly, smart device functions, applications and training features that, by incorporating cultural themes and attributes, will aid vulnerable and underserved users to securely navigate online while protecting their privacy and identity.

In order to empower an underserved or vulnerable user to engage with needed services, we must be prepared to demonstrate measured success, hence the need to create guidelines and capabilities with unique design approaches, incentives and dynamic training methods to build a trustworthy accountable messaging process so users can have a say in their data management with accountability. This mission will provide data as well as the ability to dissolve existing systemic barriers and bottlenecks faced by vulnerable and underserved populations.

The Healthcare Industry and Banking/Finance are two of the largest industries that experience the major problems from underserved and vulnerable populations and should be high priorities for the scope of work. This should not exclude other areas where secure, trusted online commerce is essential to societal well-being and advancement.

**(3) B SCOPE –** Tools

1. Publish Use Case for Trusted Identifiers for underserved populations
	1. Emphasize, highlight and prioritize user scenarios/stories from vulnerable and underserved populations to improve services for all users
	2. Test the Use Case and user stories across different verticals and persons of varying backgrounds and cultures
2. Harmonized vocabulary/dictionary
	1. Understandable by individual/common knowledge
		1. Crosswalk of W3C data privacy vocabulary or similar taxonomies vs human centric/plain language
		2. Could be a combination of plain language and metaphor/semiotics
3. Classes of Identifiers
	1. It may be necessary to create separate classes of Identifiers for selected, large, regulated industries, e.g., Finance/Banking and Healthcare among others
	2. With funding of the infrastructure law, billions of dollars are tagged to subsidize broadband high-speed internet (AT&T, Verizon and a growing number of ISPs and utilities), to millions of unconnected households, at $30 per month, in rural America. This funding will enhance the reaching in providing access to the underserved. Lowering the barrier to adoption benefits this WG mission, but it will generate a need for a unique ISP identifier matrix of some type that would link to the regulated sectors of first responders, financial/banking, education through 12 and healthcare.
4. Liaise with Kantara ANCR WG on transparent and proportional notice of risk
	1. Identifies and captures activity of data controller; exposes surveillance and enables individuals to take action

**(4) DRAFT TECHNICAL SPECIFICATIONS:** *List Working Titles of draft Technical Specifications to be produced* *(if any), projected completion dates, and the Standards Setting Organization(s) to which they will be submitted upon approval by the Membership.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Specifications in scope** | **Details** | **Dates** | **Contributed Towards** |
| TBD |  |  |  |

**(5) DRAFT RECOMMENDATIONS:** *Other Draft Recommendations and projected completion dates for* *submission for All Member Ballot.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Description** | **Link** | **Spec input summary** | **date reviewed** |
| Guidelines and Use case |  |  |  |  |

**(6) LEADERSHIP:** *Proposed WG Chair and Editor(s)*

* Chairs & Secretary (initial)
	+ Co-Chairs – Jim Kragh and Dr. Tom Sullivan
	+ Vice Chair – Catherine Schulten
	+ Secretary – TBD
	+ Editor – Noreen Whysel

**(7) AUDIENCE:** *Anticipated audience or users of the work includes*

**Community, Business ,Government leaders SW developers, vendors, security and privacy advisors**

The ultimate goal of the WG is to provide the coordination, leadership, and technical support necessary to ensure widespread adoption of a Trusted Identity Ecosystem Framework across the entire community of individual persons who need these digital credentials and online access to help reduce their vulnerability to the many adverse events of our 21st century life. To this end, we will embrace communities already engaged with vulnerable and underserved populations, along with a select few corporate entities. By engaging with them and achieving some successful measured benchmarks we will be able to influence policy-makers, thought leaders, government agencies, and private sector entities through education and advocacy. To this end the work group deliverables will address the following audiences:

* Software developers, product managers, user experience designers, information architects and others, as a means of achieving accessibility and interoperability across a wide range of identity, security, and privacy of use cases.
* Developers of decentralized governance and next generation internet services.
* Regulators looking for technical controls and solutions to implement legal requirements that scale. In particular to identify gaps in current solutions that ignore or discriminate against vulnerable and underserved populations.
* Operators of identity, privacy, security and interoperability of EHR, disaster relief and similar systems in the real world.
* Nurses, case managers, NGO program managers, teachers, physicians, social workers, librarians and other professionals who serve the needs of the underserved, provides something that can be understood by people.

**(8) DURATION:** *Objective criteria for determining when the work of the WG has been completed (or a statement that the WG is intended to be a standing WG to address work that is expected to be ongoing).*

The first phase is the completion of the use cases and in parallel the harmonized vocabulary. As in the table above this is expected to take 1 year , but there is no proposed time limit on the group.

**(9) IPR POLICY:** The Organization approved Intellectual Property Rights Policy under which the WG will operate.

Kantara Initiative IPR Policy - Patent and Copyright, Reciprocal Royalty Free, opt out to RAND,
https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=41025689

**(10) RELATED WORK AND LIAISONS:** *Related work being done in other WGs or other organizations and any proposed liaison with those other WGs or organizations.*

Developing off of the prior work of the Federated Identifiers for Resilient Ecosystems work group (FIRE WG) and the Health IT Assurance work group (HIA WG), the RIUP WG will liaise with the following work groups and organizations:

* HHS ONC (Office of the National Coordinator)
* CARIN Alliance
* FHIR HL7
* Kantara Alliance Working Groups
	+ ANCR WG
	+ PEMC WG

**(11) CONTRIBUTIONS (optional):** *A list of contributions that the proposers anticipate will be made to the WG.*

**(12) PROPOSERS:** *Names, email addresses, and any constituent affiliations of at least the minimum set of proposers required to support forming the WG. At least 3 proposers must be listed. At least 2 of the proposers must be Kantara Initiative Members -* *current members list*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Proposers Name** | **Email** | **Organization (or Individual)** | **Voting Member** | **Affiliations** |
| Jim Kragh | Kragh65@gmail.com | Individual | x |  |
| Dr. Tom Sullivan | Tsullivan@drfirst.com | Individual | x | Dr. First |
| Catherine Schulten | Catherineschulten@yahoo.com | Individual | x | Walmart |
| Noreen Whysel | Nwhysel@gmail.com | Individual | x | Decision Fish LLP |

Addendum:

**A VP Trust Framework, starts with an Authenticated Identity**

According to Pew Research, April 2021, 97% of Americans own a phone, 19%, with an income below $30k, had a cellphone and 75% had a smart phone; between the ages of 18-64, 90% had smartphones; 61% of seniors over 65 had smartphones. A majority of the vulnerable and underserved population have smartphones for social purposes; not state issued ID or authenticated identifiers and not trust framework platform.

**Trust Framework Features and Functions**

(Scalable, flexible and mitigates risk)

**Features**: Currently we are now and, in the future, will be living in an “always on and connected” framework of platforms with end points, human devices, and software-applications that generate data (assets) initiated by a user ID/identifier.

**Functions**: Users ‘access’ data-assets using technologies that initiate a process in a defined environment that is governed by privacy rules and a policy engine.

**Elements** of an AAL/IAL onramp for a trusted identity/identifier. The engagement may be a combination of assurance features like attributers, a verification and validation process, possession of a device/key, a unique credential or a biometric the combination of which initiate authentication, authorization and privacy functions.

To protect your identity, privacy and data, start with building your **trusted** online identity. For a VP user, would enroll for a base level **trusted authenticated identity** with a receipt feature and be given a beneficial valued incentive. An enrollee seeking a strong online **high** **trust level** authenticatedidentity with digital signing and a non-repudiated functions andreceipts features in addition to a valued incentive.

Kantara’s tools: (including FIRE & HIA docs sent to ONC)

* Federated identity and Identity and Assurance = Privacy
	+ Credentials, Policies and Access Controls
	+ Identifiers and Matching
	+ User Relationships and Exchanges
* Digital notice and Consent-Receipts
* Smart Mobile Devices / Endpoints
	+ EHR interface, HL-7/Smart-on FHIR, APIs
	+ Data Aggregation, User Data Management
* A Kantara **Trustmark** for Vulnerable and Underserved Populations

The Vulnerable and Underserved Populations should not experience any barriers to access beyond those that privileged claimants also face. (according to ADA)

**A Trust Profile of terms:**

According to a national accounting firm, technical **trust** is “a set of enterprise technical attributes that helps deliver a positive customer experience.” We believe that ‘**trust’** a confidence that one has in another that the second will behave as expected. **Trusted**, indicates that one element relies on the other to fulfill a requirement on its behalf. Technically, a **‘trusted boot’** (NIST) is a system boot where aspects of the hardware and firmware are measured and compared against known good values to verify integrity and **trustworthiness;** it represents that the technology is worthy of beingtrusted to fulfill the requirement. A **Trustmark** is an official seal, authentication feature, certification, license, or logo provided by an identity trust framework operator to certified identity providers within its identity trust framework or federation to signify that the identity provider complies with the written rules and policies of the identity trust framework or federation.