

# The Kantara Initiative Value Proposition for the Electronic Healthcare Modernization

November 29, 2012

## **Introduction**

Thank you for providing the opportunity for Kantara Initiative to offer testimony and suggestions regarding Electronic Healthcare and, in particular, Patient Identity Proofing and Authentication.

My name is Joni Brennan and I am the Executive Director of Kantara Initiative. It's my honor and pleasure to speak with you today representing all Kantara Initiative stakeholders.

Kantara Initiative is a non-profit 501c6, member driven organization providing a neutral forum for the harmonization of authentication policies and technologies with multi-stakeholder engagement from public sector, private industry and research and education network stakeholders. The Kantara Initiative develops and verifies trust framework criteria based on requirement considerations for: policy, technical, and privacy practices.

Kantara Initiative has over 80 members and partners representing national and international interests to build and verify Trusted Identity Ecosystems across varying sectors including: government agencies, healthcare, telecommunications, financial, and eCommerce. Kantara Initiative has strong healthcare industry representation with members including organizations like: ApeniMed, SureScripts, HIMSS, eHealth Ohio, Probaris, SecureKey and SAFE-BioPharma. Note that while we would like to highlight every member and participant of Kantara Initiative as they are each integral to our success, in the interest of time we've provided a sample here and the full list of members, liaisons and partners is available from our website.

Kantara Initiative operates over 10 active working groups and, in particular, the Health Identity Assurance Work Group (HIAWG) provides a focus group to advance Identity Management policy and technology enhancement and convergence. The HIAWG is lead by Pete Palmer of SureScripts, John Fraser of ApeniMED, and Rick Moore of eHealth Ohio. The HIAWG includes participants such as: Global Patient Identifiers, Inc., Experian Healthcare, American Academy of Family Physicians, Park Avenue Capital dba MaxMD, Anakam, LifeMed ID, Inc., eHealth Ontario, AETNA, MedCommons, CIGNA, Gemalto, Blue Cross of Idaho, and Probaris. Additionally, Pete Palmer of SureScripts chairs the Kantara Initiative Leadership Council, a council consisting of all Kantara Initiative leadership.

## **Setting the Stage - Electronic Healthcare Landscape**

There are numerous initiatives evolving in the health care sector that require strong identity management to ensure security, privacy, and trust. These include the many Health Information Exchanges (HIEs) being deployed around the country, DirectTrust.org, the Drug Enforcement Agency's electronic prescribing of controlled substances (EPCS) rule, the Nationwide Health Information (NwHIN) development, Accountable Care Organization (ACO) pilots, and "meaningful use" interoperability requirements. The Trust Framework programs of the Kantara Initiative provide the basic elements

needed to verify trust in Identity Ecosystems components where a single identity can be used and re-used in these and numerous other healthcare scenarios.

Today, a health care provider's identity is tied to each clinical and administrative system they use. Single sign-on solutions exist for some large organizations, but these solutions do not necessarily scale beyond the walls of the organization. In this 'extended' environment, point-to-point integration and agreements must exist between organizations in order to provide system access to individuals. This requires health care providers to manage a multitude of credentials to access their various accounts for clinical and administrative data exchange.

Individual health care providers need solutions that are portable and ubiquitous, while health care provider organizations, such as integrated delivery systems, need assurance that their affiliated health care providers have adequate trust to access services and information regarding their mutual patients. Health IT system vendors need standard policies and technologies to minimize their operational cost while maximizing options for their customers.

Patients need trusted, safe, secure, interoperable, and easy-to-use credentials to access their electronic health records. However, such patient credentials must not compromise security for convenience. Rather, the identity vetting and credential management of patient credentials must be scaled to appropriately match information transaction context and risk assessment. Security itself must never be mitigated but means and methods to achieve higher levels of assurance can be comprised of comparable solutions that meet the need for identity assurance in innovative ways. We are already seeing the development of 'layered' type approaches to elevation of trust in an authentication using verifiable attributes for example.

### **Overview - The Kantara Initiative Approach**

With origins in the Electronic Authentication Partnership (EAP) the Kantara Initiative Identity Assurance Framework (IAF) was developed over the past 10 years in order to provide a standard, well understood methodology for issuing and managing trusted digital credentials in support of identity management.

The IAF and the federal government's NIST 800-63 standards have been harmonized and support the following to ensure identity trust and interoperability:

1. Four progressively stronger levels of assurance
2. The identity proofing requirements for each level of assurance
3. The types of credentials that can be used at the various assurance levels
4. The acceptable methods for authenticating these credentials

### **Operating Now - Kantara Initiative Trust Framework Programs**

The US GSA Federal Identity Credential Access Management (FICAM) team has selected Kantara Initiative to operate as a Trust Framework Provider (TFP) verifying Credential Service Provider services at

Levels of Assurance 1 – 3 non-crypto. Effectively this means that, under the FICAM program, a Kantara Initiative “Service Approval” enables US Government agencies to trust and consume credentials that are proofed, issued and managed by private sector Service Approved organizations.

The Kantara Initiative Accredited Assessor ecosystem includes: Deloitte & Touche, Electrosoft, eValid8, Europoint, and Zygya. Our Approved Credential Service Provider is Verizon Universal Identity Service (LoA 1-3 non-crypto) with 8 other organizations in queue for Service Approval including Daon Inc., a new member of Kantara. Additionally, Kantara Initiative is pioneering a new approach of Component Service Recognition with Experian Precise ID (LoA 2,3) as the first Kantara Recognized Identity Proofing Component.

We are excited to formalize a Component Service approach for Identity Proofing and Credential Management organizations. Our next step will be to explore the standardization of integration of Component Services. This approach will truly enable a Component Service “plug and play” environment and provide opportunities for trusted industry organizations to partner in new and innovative ways with speed to market. Finally, the Component Service approach will enable a stepped approach to Identity Federation Ecosystem adoption allowing Relying Parties (organizations which consume “third-party” trusted credentials) the ability to shift away from scenarios where Service Providers also act as Identity Providers toward models for adoption where Service Providers outsource all or some of Identity Management features. Note that, while this program is able to scale and expand to verify trust in varying Identity Ecosystem components, it currently focuses specifically on single user credentials (for example that of patients or doctors rather than that of entities or devices).

Kantara Initiative works closely with industry stakeholders to identify, mitigate and resolve gaps identified with regard to industry alignment with the spirit and intent of government based requirements like that of NIST Special Publication 800-63. Kantara Initiative uses open and transparent vendor neutral consortia based governance to ‘bridge the gap’ between public and private sector communities for the good of Identity Ecosystems actors at-large. Thus Kantara Initiative truly supports and fosters partnerships of all kinds including public-private initiatives.

### **Collaboration and Community - Working Together Toward Harmonization**

Kantara Initiative has as a core value the desire to work collaboratively to harmonize Identity Management Authentication and Access solutions to enable frequent use and re-use of trusted digital credentials while maintaining appropriate levels of security and assurance based upon risk context.

Kantara Initiative has been consulted through the development process of the National Strategy for Trusted Identities in Cyberspace (NSTIC) and has also been sought out by NSTIC Pilot organizations including Daon Inc. for Kantara Service Approval and by Resilient Network for policy and governance practices review by Kantara policy and governance Subject Matter Experts.

Kantara Initiative focuses not only on the US Government scenarios but on a pan-jurisdictional scale via active liaison relationships with organizations including the International Organization for Standardization (ISO) and International Telecommunications Union – Telecommunications

Standardization (ITU-T). Kantara Initiative also has active engagement on an international scale including that of the Internet Society (ISOC), Nomura Research Institute (NRI, Japan), Government of Canada, New Zealand Government Department of Internal Affairs and Trans-European Research and Education Networking Association (Terena).

Most recently we are pleased to share a memorandum of understanding between Kantara Initiative and DirectTrust.org.

Recognizing that there are numerous initiatives evolving in the health care sector that require strong identity management to ensure adequate security and trust of health information transported over the Internet, DirectTrust.org and the Kantara Initiative seek a collaboration that will help to minimize the development of "silos" of non-standard and unrelated identity vetting process and documentation. Both organizations seek to help provide the common and basic elements needed to support a single health Internet/cyberspace identity to be broadly used by health care professionals as they obtain a variety of online credentials.

Kantara Initiative has the mission to foster identity community harmonization, interoperability, innovation, and broad adoption through the development criteria for operational trust frameworks and deployment/usage best practices for privacy-respecting, secure access to trusted online services. The Kantara Identity Assurance Framework (IAF) provides many of the basic elements needed to support a trusted identity ecosystem that could enable a single identity to be used in these and numerous other health care scenarios. In addition to developing the IAF and other frameworks, Kantara Initiative is a Trust Framework Provider (TFP), for the US Government, working to gather requirements for trusted identity credentials in verticals and jurisdictions.

DirectTrust.org is a non-profit industry coalition that is providing security and trust policies and best practice recommendations in support of scalable growth of Directed health information exchange. The DirectTrust.org X.509 Certificate Policy aims to provide clarity, transparency, and choice in the levels of identity assurance relied upon for issuance of credentials used in Direct message exchanges, characteristics which are needed for scalable and federated trust to flourish within the Direct community. DirectTrust.org is jointly developing with EHNAC an Accreditation Program for HISPs, CAs, and RAs who act as Trusted Agents in the implementation and delivery of Direct exchange services, based in part upon the DirectTrust.org Certificate Policy.

Thus, it is natural that DirectTrust.org and the Kantara Initiative seek to collaborate in order to align each organization's efforts toward the common goal of interoperability of trusted identity credentials within the health care identity ecosystem to the extent possible, and with the recognition that the Federal government is providing governance, policy, and regulations as a framework within which we all must cooperate (e.g., the FICAM, FBCA, and NSTIC).

### **The Kantara Initiative Offer**

Kantara Initiative offers our Trust Framework Provider programs for adoption by varying cross-vertical end-user communities. Our programs are operational and managed by world-wide experts in the fields

of: Identity Management, Federation Operators, Government Policy Makers, Assessors, Service Providers (Relying Parties), and Research and Education Networks. One of our main goals is to ensure that organizations and communities do not need to reinvent the wheel to perform such services. Kantara continually collaborates with partners and peers to provide a set of high value trusted services to end-user stakeholders.

We invite all types of stakeholders to join our discussions and we are pleased to join discussions in other venues as well. We feel that collaborations support the advancement of industry achievements in a way that mutually benefits diverse communities with shared interests.

## **Conclusion**

The Kantara Initiative, its members and partners, include diverse and unique subject matter experts. Kantara Initiative Trust Frameworks are operational and, today and in the future, our programs play a vital role in ensuring the success in the healthcare sector as it transitions from the paper to digital world. Use of these proven methodologies can enable rapid, efficient, cost-effective and error-free achievement of the identity and trust infrastructure required by the emerging generation of healthcare automation. Thank you for allowing Kantara Initiative to participate in this virtual hearing. Further information about Kantara Initiative, a full list of members and partners and recent Services Approved can be found at [www.kantarainitiative.org](http://www.kantarainitiative.org) and we would be happy answer any questions and to participate in any follow on discussions.