April 9th, 2021

Attn: NIST Computer Security Division, Information Technology Laboratory

This response is submitted by Kantara Initiative Inc.

Kantara is the leading global consortium whose mission is to grow and fulfill the market for trustworthy use of identity and personal data. To fulfill this mission Kantara operates an independent third-party conformity assessment program for the digital identity and personal data ecosystems as well as providing real-world innovation through its development of specifications, such as UMA 2.0, Consent Receipt, applied R&D, its Identity Assurance Framework (IAF).

This submission was developed by participants in Kantara's Identity Assurance Work Group (IAWG). The IAWG consists of individuals from both the public and private sectors with extensive experience in the identity industry including assessing identity services for conformance to established requirements, developing requirements for identity services, and implementing and providing identity related products and services.

If you would like to further discuss the following inputs, please contact us at secretariat@kantarainitiative.org

Sincerely,

Ruth Puente

Ruth Puente

Director, Assurance Operations
Kantara Initiative Inc.
www.kantarainitiative.org

Kantara Comments on NSTIR 8344 Ontology for authentication

Purpose of the Document

Kantara is unsure of the purpose of this document.

While the Introduction of the document identifies what the document contains, it does not identify why the document is needed. For example, how does it relate to SP800-63 or other NIST publications? Would Kantara be correct in assuming that it provides the foundation upon which the requirements identified in SP800-63 have been developed?

Definitions

In order to maximize the possibility of interoperability with other federations, Kantara would recommend that the definition of terms be based, as much as possible, on definitions from existing standards. Kantara would suggest that, when NIST finds those definitions to be inadequate, the document be used to discuss why the definition of a term is inadequate and propose a new definition. Kantara would also suggest that definitions include real world examples to further the understanding of a term.

The definition of Ontology provided in the document is: "Defines the organization, structures, properties, and interrelations of a complex idea or construct." Kantara suggests that, while this definition implies "in a subject area", it be made explicit in the definition. As such, Kantara recommends the following definition: "Defines the organization, structures, properties, and interrelations of concepts in a subject area."

While the definition of Ontology states that it defines key concepts and their interrelationships, Kantara would suggest that the current Ontology falls short for several key core concepts. For example, the concept of Federation and Trust Framework are not discussed. Kantara would suggest the following terms be included:

- Trust Framework: the set of requirements and enforcement mechanisms governing participants in a Federation (adapted from ISO 29115). A Federation defines its Trust Framework. A Trust Framework can, but does necessarily need to, be part of a Federation Agreement.
- Federation: two or more domains that want to interact (adapted from definition of Identity Federation Agreement in ISO 24760). For example, the Credit Card Federation consists of all those that want to use credit cards to effect payments for goods and services. That is, buyers, sellers and financial institutions. A Federation is responsible for

developing, maintaining and enforcing a Trust Framework. A Federation is governed by a Federation Agreement.

- Federation Agreement. The rules and processes that enable participants in a Federation to interact (adapted from definition of Identity Federation Agreement in ISO 24760).

Kantara found other, what it believes are key, terms throughout the document that were not defined. Kantara would recommend that the following terms be defined and discussed in the Ontology:

- Entity: any concrete or abstract thing of interest (ISO 10746)
- Object: Is object synonymous with entity?
- Trust: this term underlies many of the concepts. In Kantara's opinion, Trust is a function of predictability or reliability and is based on a level of risk. Kantara would suggest the following definition for Trust: The extent to which something behaves as it is intended to behave. (adapted from the definition of Trust in ISO 13888-1)
- Risk: management of risk and risk tolerance also underlie many of the concepts. Kantara would suggest the following definition for Risk: A combination of the probability of occurrence of harm and the severity of that harm. (from a variety of ISO standards including 27809, 13702, and 15188)

Kantara also finds some of the definitions are circular. For example, the document provides the following definition for Authentication: "One of the steps in the IAA process: identify, authenticate, and authorize. A component of the IAA process in which a token is tested." The Oxford dictionary defines Authentication as: "the act of proving that something is real, true or what somebody claims it is." Based on this definition, Kantara recommends the following definition for Authentication: "the act of proving that something is real, true or what somebody claims it is." This definition is consistent with the definition of Identity Authentication found in ISO 29115. Kantara would also suggest adding the following as notes to this definition: "Authentication is one of the steps in the IAA process: identify, authenticate, and authorize. During Authentication somebody proves to someone who requires the proof that they are who they say that they are." In addition, Kantara suggests that the document discuss the concept of reauthentication including whether re-identification is required.

Kantara is also concerned that some of the examples that have been provided in the document may confuse, rather than enlighten, readers if they are not already experts. For example, PKI is not simply a form of digital signature, certificate authorities are not familiar to the uninitiated, and the mention of blockchain will not enlighten those unfamiliar with digital signatures, let alone electronic signatures.

Kantara would recommend that terms in the document be presented in relational, rather than alphabetical, order. That is, terms and concepts are presented respecting the rule that no terms or concept may use another defined term unless it has been previously defined. This serves to provide a 'developing comprehension' as definitions are read-through in a developing 'story-line'. This also serves to ensure that, importantly, there are no circularities within the definitions.