Kantara Initiative Identity Assurance Framework --

Validating Trustworthy Identity Ecosystem Components

Version dated: 25 July 2012

Target document: IAWG Report

Identity ecosystems around the world continue to crystalize, and, as they do so, the number of applications that rely on their effectiveness and validity is increasing dramatically. Functions such as identity verification and credential authentication, which were traditionally fulfilled within a closed-enterprise identity lifecycle, are now being provided in modular service components that can support a wide range of applications, i.e. e-Government, health care, and financial. The Kantara Identity Assurance Framework (IAF) states the generic Identity Assurance and Privacy Safeguards requirements for Identity Ecosystem components. The Kantara Assessment program uses the IAF to accredit Assessors and to validate Service Providers. Thus, the Kantara Identity Assurance Framework (IAF) and associated programs provide a mechanism for the independent validation of the trustworthiness of identity system components, as recognized by such parties as the US CIO FICAM sub-committee. This is a crucial step in ensuring that the security and privacy considerations for a wide array of business objectives are met, in an online environment.

Background

As identity ecosystems evolve to support a broad number of applications, the historically sequential chain of functions, such as: user provisioning; identity verification; credential authentication; and entitlement authorization; are being implemented as modular services. The *modularization* of these functions into service components enables their sharing across the multiple relying parties. In addition to the economic benefit of sharing such services, the other two reasons for modularization are: to avoid unnecessary proliferation of personal data (by limiting the number of points at which a user provides personal data); and to support requirements for segregation of functions such as identity verification and entitlement authorization. This permits more program flexibility and a migration from traditional built-in identity proofing to a system based on services provided by a number of trusted suppliers.

As this shift of the underlying architecture for identity systems moves from the sequential enterprise framework, where trust was delegated down through each function, to a federated identity system of interconnected components, the *trustworthiness* of each constituent component becomes paramount. This requirement for trustworthy components places a higher degree of scrutiny and accountability (business and technology) on component technologies than was previously exposed in a sequential-system flow of trust. In addition to component trustworthiness, a viable identity ecosystem also requires consistency (i.e. commensurate processes and policies) across all service components, for considerations such as privacy safeguards for data at rest and transport protection for data in motion. The Kantara Identity Assurance Framework was developed by a broad

range of international identity and privacy experts and so reflects a wide set of considerations that would determine such service provider consistency.

Trustworthiness can be demonstrated in a couple of key ways: the underlying framework for an identity ecosystem can be demonstrated as trustworthy by an examination of the operating procedures and policies; and each of the service components can be validated to provide a specific level of service, via a component assessment scheme.

Kantara Initiative Identity Assurance Framework

The Kantara Initiative Identity Assurance Framework (IAF) was developed to satisfy both of these key elements of identity system trustworthiness. The IAF traces back to e-authentication initiatives described by OMB-04-04[1] and its supporting NIST Special Publication 800-63[2]. These documents define the requirements for identity assurance at specified degrees of risk, and provide the basis for the operating conditions for service components in the current version of the IAF[3]. As such, the IAF supports the four levels of assurance that are generally recognized (albeit with different terminology) by the governments of the U.S.[4], Canada[5], UK, New Zealand and others regions, such as the EU[6].

The current version of the Identity Assurance Framework supports a modular approach down to the level of separating out the functions of identity verification and credential authentication. This de-coupling of identity from credential authentication allows a wide range of identity ecosystem implementations to be accommodated. As an example, in some jurisdictions, privacy legislation requires that identity verification to support a claim of entitlement is only executed at the point of service delivery, and not be implied in a transported credential.

In terms of service components, trustworthiness typically comprises demonstration of two significant factors: that the operational processes and procedures of the component are sufficient to support the degree of asserted identity assurance; and that the underlying security safeguards for data protection are sufficient.

IAF Maintenance and Development

The Kantara IAF states the generic requirements for such Identity Assurance and Privacy Safeguards. The Kantara Assessment program provides for the Accreditation of Assessors and the validation of Service Providers. The detailed Assessment Criteria for such validation of Service Providers is maintained by the Kantara Identity Assurance Work Group (IAWG) and the Kantara Privacy and Public Policy Work Group (P3WG), for Identity Assurance and Privacy Safeguards, respectively.

The Kantara IAF was designed to be as generic as possible and thereby intended to support a range of identity initiatives “out of the box”. Sector-specific nuances or instantiations of the Identity Assurance Framework, for example, to accommodate varying government, health care, or telecommunications industry requirements are documented in profiles of the IAF. These profiles are coordinated by the respective Kantara Work Group (eGov, Health Care ID, Telco ID) to the IAWG and P3WG. This allows the overall Kantara IAF to support a broad range of government, health care, financial, and telecommunication sector embodiments.

As an example of a sector-specific embodiment of the IAF, there are numerous initiatives evolving in the health care sector that require strong identity management to ensure adequate trust. Some examples in the U.S. include the many Health Information Exchanges (HIEs) being deployed around the country, the Drug Enforcement Agency's electronic prescribing of controlled substances (EPCS) rule, ONC's Direct effort, the Nationwide Health Information (NwHIN) development, Accountable Care Organization (ACO) pilots, and "meaningful use" interoperability requirements. The Kantara Identity Assurance Framework and associated Assessment and Accreditation Schemes provide all of the basic elements needed to support a trusted identity ecosystem that enables a single identity to be broadly used in these and numerous other health care scenarios.

Summary

The Kantara Identity Assurance Framework provides an independent mechanism to establish the trustworthiness of identity components to support a wide range of applications, in an effective and validated manner. This will reinforce user acceptance of such applications by establishing clear definitions of identity assurance processes and the steps taken to protect personal data.

References

[1] E-Authentication Guidance for Federal Agencies
www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

[2] Electronic Authentication Guideline Recommendations
csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[3] Kantara Identity Assurance Framework
http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework+v2.0

[4] National Strategy for Trusted Identities in Cyberspace
http://www.nist.gov/nstic/

[5] Cyber Authentication Renewal Initiative
http://www.tbs-sct.gc.ca/sim-gsi/si-is/docs/ident-eng.asp

[6] European STORK project on a European eID Interoperability Platform
https://www.eid-stork.eu/