High level Description: Kantara Conformity Assessment and the role of the Assurance Review Board

(to be read in conjunction with Kantara's Assurance Trust Framework Operations Program documentation)

Kantara Assessment model

Granting Approvals to Credential Services is the *raison d'être* of Kantara Initiative's Identity Assurance Framework (IAF). Even though Accreditation is an equally formally-administered process, it is but a means to an end, that end being to ensure that Assessments on which Approvals are based have been conducted by suitably qualified and competent organizations and persons, thus underpinning the Assurance given by the IAF.

The Kantara IAF's assessment model is based on established best practice as defined in ISO/IEC 17065:2012 "*Conformity assessment — Requirements for bodies certifying [...] services*" [IS17065], which allows for annual reviews to be less demanding than the initial assessment, subject to the three-year cycle being re-commenced when the Grant of Approval is renewed on the third anniversary of it being last granted (or reset).

Assessments are performed by Accredited Assessors who are tasked with determining a service's conformity to the selected Service Assessment Criteria (SAC). The available sets of SAC are described at https://kantarainitiative.org/trustoperations/classes-of-approval/ . SAC may cover a range of assurance levels and the applicable management and organizational practices. Depending upon the nature of the and the selected SAC(s) (e.g. the assurance levels at which it is offered– assuming the selected has such; the range of functional capabilities which it provides; the Credential Service Provider (CSP) may select a sub-set of the full criteria, based upon the scope of its offering.

At the outset of the process, each service articulates a 'Statement of Conformity' (SoC) that defines the actual criteria from the selected SAC(s) that the CSP's service seeks conformance to and that the CSP's service must be found to be conformant to, in order for it to be considered for Grant of Approval.

Approval is granted against a specific scope (in terms of the specification of the service and the applicable criteria), on the basis of on-going conformity with the terms of Approval and operation.

After the CSP provides the scope of the assessment by stating in the SoC which set of SAC is applicable to its service and therefore it has a reasonable assurance that can demonstrate conformity to that SAC set, an Kantara Accredited Assessor contracted by the CSP conducts a technical/operational and business and organizational conformity assessment which could include the following:

- Clinical review of the service and review evidential documentation: Perform testing of the assertions in the Specification of Service Subject to Assessment and the Statement of Conformity according to specific methodology based on ISO standards and best practices, following the requirements of the Identity Assurance Framework Service Approval Handbook.
- Determine if the CSP maintains effective controls over operations, set forth in Credential Policy and Credential Practices Statement, Statement of Conformity requirements decomposition and conformity evaluation.
- Review if the CSP has proper processes and procedures that ensure the provider organization's good standing and management/operational practices.
- On-site visits: Review of site/facilities, observe practices; Conduct interviews with key staff associated with the service's management, development, operation and supporting corporate infrastructure office data centers/offices;
- Review remotely incident management handling, vulnerability management, risk management, procedures, logs and records.
- Raise any non-conformity observed and evaluate if the remediation plan and timeline is acceptable.
- Determine if the CSP service is conformant with the criteria set forth in the referenced Statement of Conformity at the claimed Assurance Levels.

Risk Assessment vs. Kantara Conformity Assessments

Enterprises should perform risk assessments in order to understand what threats might imperil the assets (as defined by the scope of the risk assessment) which the enterprise seeks to protect. After consideration of vulnerabilities which the threats might exploit, together with the likelihood of occurrence of these perceived threats and the value (absolute or relative) of the assets in question, the enterprise can identify a set of counter-measures it may wish to deploy and from that list select and implement the measure(s) most likely to give the best return on investment.

Kantara grants Approval for services which have been found to be conformant to a set of Kantara-defined criteria typically specific to a particular standard or specification for which a service provider seeks evidence of compliance. These criteria are quite broad yet focused on the operation of identity proofing and credential management functions, for a given level of assurance. The criteria used address not only the technical functionality of the target service but also the service provider's *bona fides* together with the information security management practices which it applies in the operation of the service. One such expected practice is evidence of the performance of a risk assessment to help the service provider put in place the counter-measures (also known as 'controls') necessary to protect the provision of the service and the sensitive personal information to which it must have access.

Kantara lists independent third parties (Accredited Assessors) which it accredits as being competent to perform the task, carry applicable insurance etc. When contracted by the applicant service provider seeking Kantara Approval, the Accredited Assessor assesses the conformity of the service provider and their services. The independence of these Assessors, as well as the appropriateness of the criteria against which they assess, helps to underpin the value in the assurance given by a Kantara Approval.

Indeed, organizations procuring an identity proofing and credential management service should perform their own risk assessments around their use of a service in question, and should use the assurance provided by the independence of Kantara and its Assessors as one of their risk mitigation controls.

Assurance Review Board

The Assurance Review Board (ARB) is the operational authoritative body of the Kantara Trust Framework Operations Program (TFOP). The ARB receives its operational mandate from the Kantara Board of Directors that is applicably insured for the scope of its remit.

The ARB is composed of subject matter experts from a range of fields applicable to the Assurance of identity proofing, credential management and Authentication services, in accordance with its Charter.

The ARB is responsible for the day-to-day management and operation of the IAF. Its principal functions are the accepting and reviewing of applications for Approval and for Accreditation, and in making recommendations to the KIBoD for the granting of these respective Trust Marks. The ARB is also responsible for monitoring the ongoing approval and accreditation activities as well as making recommendations for improving the overall approval program.

In accordance with the IAF, the ARB creates and executes review plans relevant to applications and reports regarding Assessor Accreditation and CSP Approval. For CSP applications, the ARB performs due diligence processes and procedures to examine the approval application package for a specific Class of Approval, including the Kantara Assessor's Report (KAR), Specification of a Service Subject to Assessment (S3A), Statement of Conformity (SoC). If recommended for approval, it provides recommendations for Trust Mark Grants of Rights of Use to the main Kantara Board of Directors (to grant unconditionally; grant conditionally (i.e. that the application will be reviewed in no less than 6 months; or reject with justification). In the case of an appeal against the rejection or qualification of an application, for recommendations originating with the ARB, three additional ad-hoc members serve on the ARB to review the recommendation and make a final determination, within two weeks of an appeal being filed,.

The ARB members maintain confidentiality and impartiality throughout the life-cycle of the assessment and approval process. Moreover, they are subject to NDA procedures and recusal policy in the case of conflict of interest.