Identity Assurance Framework:
Rules governing Assurance Assessments

Version: 1.0*bis*

Date: 2013-02-07

Status: Final Recommendation

Approval: KIR20130207

Editor: Richard G. Wilsher
Zygma LLC

Contributors: https://kantarainitiative.org/confluence/x/k4PEAw

Abstract

The Kantara Initiative Identity Assurance Work Group (IAWG) was formed to foster adoption of identity trust services. The primary deliverable of the IAWG is the Identity Assurance Framework (IAF), which is comprised of many different documents that detail the levels of assurance and the certification program that bring the Framework to the marketplace. The IAF set of documents includes an Overview publication, the *IAF Glossary*, a summary *Assurance Levels* document, and an *Assurance Assessment Scheme (AAS)*, which encompasses the associated assessment and certification program, as well as several subordinate documents, among them these *Service Assessment Criteria (SAC)*, which establishes baseline criteria for general organizational conformity, identity proofing services, credential strength, and credential management services against which all CSPs will be evaluated.

The latest versions of each of these documents can be found on Kantara's Identity Assurance Framework - General Information web page.

Notice:

47 # CONTENTS
48
49 **1 INTRODUCTION 4**
50 1.1 Status and Readership 4
51 1.2 Purpose 4
52 **2 GLOSSARY 5**
53 **3 SELECTION OF SERVICE ASSESSMENT CRITERIA 6**
54 3.1 Principles 6
55 3.1.1 Statement of Conformity 6
56 3.1.2 Service Component Assessments 6
57 3.1.3 Full Service Assessments 7
58 3.1.4 Period-of-Time versus Day-Zero Assessments 8
59

1 INTRODUCTION

1.1 Status and Readership

This document sets out **normative** Kantara requirements and is required reading for all Kantara Accredited Assessors and applicant Service Providers. It will also be of interest to those wishing to gain a detailed knowledge of the workings of the Kantara Initiative's Identity Assurance Framework.

1.2 Purpose

The ultimate goal of the Kantara Initiative's Identity Assurance Framework (IAF) is the facilitation of intra- and inter-Federation transactions based upon a range of identity credentials, across a number of levels of assurance, in which Relying Parties can have the confidence that the credentials bearing the Kantara Initiative Trust Mark are worthy of their trust.

To accomplish this Kantara Initiative operates an *Assurance Assessment Scheme (AAS)*, an assessment and approval program which assesses the operating standards of certain players in the Identity and Credential Assurance Management space against strict criteria, and grants to Applicants to the scheme the right to use the Kantara Initiative Mark, a symbol of trustworthy identity and credential management services at specified Assurance Levels (i.e. a Grant of Rights of Use – hereafter 'Grant').

In implementing the AAS certain Rules are required to be set out, to support fulfillment of the Assessment Scheme and to direct how certain actions and processes within it are bounded and executed. This present document serves that purpose and can be considered to sit between the AAS and the *Service Assessment Criteria*, to which Approved Services must conform and against which their conformity must be assessed by Kantara-Accredited Assessors.

The latest versions of each of the IAF documents referenced in this document can be found on Kantara's Identity Assurance Framework - General Information web page.

2 GLOSSARY

All special terms used in this document are defined in the *IAF Glossary*.

3 SELECTION OF SERVICE ASSESSMENT CRITERIA

3.1 Principles

Kantara's *Service Assessment Criteria* are in two classifications, Common Organizational Criteria (CO-SAC) and Operational Criteria (OP-SAC), and Services may be submitted for Approval in two classifications, as a Service Component or as a Full Service. This Section defines the rules under which Applicants for Service Approvals must be assessed and must conform to applicable criteria.

3.1.1 Statement of Conformity

The Statement of Conformity (SoC) (a document required by the *Specification of a Service Subject to Assessment – S3A*) must state, for each criterion in each SAC and at each applicable Assurance Level(s), whether the criterion is:

a) "not within scope";

b) fulfilled by another previously-Approved Component Service which is incorporated into the Applicant Service (which must be identified according to its Kanata Approval reference); or

c) is fulfilled directly by the Applicant Service, in which case the SoC must state how conformity is achieved (which may include, where justified, a statement that the criterion is 'not applicable').

Kantara prescribes the required minimum content of the SoC but not a specific structure. However, Kantara strongly recommends developing the SoC using the conformity tables provided in the *Service Assessment Criteria*. The SoC may be a stand-alone document or may be incorporated into another document if that is justified. Kantara's requirement is that a specific documented source of the required information be available and labeled as the SoC.

3.1.2 Service Component Assessments

A Service Component's SoC must identify which OP-SAC criteria are applicable (i.e. are within the service's scope) and for those criteria must state how conformity with them is achieved.

The concept of a Service Component is intended to permit flexibility with a Full Service who's CSP which may choose to operate their service core as the basis for multiple service offerings using different Service Components (e.g. to satisfy different market sectors or to permit operations in different jurisdictions). This approach allows significant flexibility in how services are

developed by no longer imposing a specific dominance of any particular aspect of the service's provision[1].

Applicants for Service Component Approval must justify the selection of OP-SAC criteria to which they have elected to conform – the ARB, in assessing an application, shall review the scope of the SoC and shall have the right to ask the Applicant to justify their scope.

The operator of an Approved Service Component is entitled to market their service as being Kantara (Component)-Approved to any parties but, where the consumer of that service is not another Kantara-Approved Service (whether Component or Full), Kantara Initiative shall make no claims, nor make any warranties, nor have any interest or liability whatsoever.

3.1.3 Full Service Assessments

A Full Service may have all OP-SAC criteria met by the Applicant itself or they may be met by the inclusion of any number of Service Components.

The Applicant's SoC must (as stated above) state which criteria (if any) are met by any already-Approved Service Components, which will be initially verified by the Secretariat on first receipt of an Application for Full Service.

The Assessment of a Full Service need not include re-examination of the conformity of Component Services being included, unless circumstances suggest there is a justified reason to do so, but must establish that:

a) all 100% of the SAC OP-SAC criteria have been addressed within the collective service;

b) where any criterion happens to fall into more than one Component, that there is a clear responsibility on the part of one specific provider that that criterion is being met or that its dual operation does not present any conflicts in the overall provision of the service;

c) there is adequate contractual specification, driven by the Full Service Provider, governing the technical responsibilities and inter-operation of the Components and evidence that that is being accomplished in reality;

[1] Previous versions of IAF-1400 SAC had assumed that the Credential Management component of an overall service would be pre-eminent.

d) the provider of each Component Service has, within the thirty (30) days preceding the start of the assessment, provided an attestation to the effect that the scope, description, operation and conformity of their Component has not materially changed[2] since the last Assessment of that Component.

The implication of the above is that a Full Service Provider may submit for Assessment and Approval a service constructed purely of previously-Approved Components (i.e. one in which the Provider making the Application provided no essential functionality whatsoever), thus making the determination of contractual arrangements fundamental to ensuring that the Components collectively deliver a Full Service.

3.1.4 Period-of-Time versus Day-Zero Assessments

3.1.4.1 Period-of-Time Assessments

It is a Kantara condition of (Full, versus Component) Approval that Services must be already operational before being subjected to an Assessment. The following periods of time are the minimum periods for which services must be operating before a Period-of-Time (PoT) assessment can commence (i.e. one addressing a period of time over which the Service has been operational and therefore has a history which can provide supporting evidence):

Assurance Level:	1	2	3	4
Minimum operational period (days)	0	30	60	90

3.1.4.2 Day Zero Assessments

Under certain circumstances CSPs may desire a Kantara Approval in advance of there being any operational history on which a Period-of-Time assessment could be based. Kantara provides for such circumstances by accepting a Day-Zero (DZ) Assessment (i.e. one in which there is no operational record to underpin the quality of the assessment) as an interim measure, conditional upon a PoT Assessment being provided within a specific period (see below).

[2] A material change would be one which required a change to the scoping statement, involved a change of functionality provided or the manner of provision of defined functionality, or which had changed to the point where conformity to any applicable SAC requirement could no longer be upheld or had been replaced by a means of conformity which had not been reviewed in the course of the Assessment on which the present Approval was granted.

CSPs which elect to seek Approval based on a DZ Assessment may submit their Application at any time at which they are able to fulfill the applicable SAC, supported by their chosen Kantara-Accredited Assessor's DZ Report, subject to the requirement that they must subsequently provide an Assessment Report based upon a PoT Assessment conformant to the operational period described above.

The follow-on PoT Assessment Report must be submitted within 180 days of the DZ-based Application, with the exception of LoA1, which must be satisfied by a PoT Assessment being performed on or before the occasion of the first annual assessment.

Failure to submit the PoT Assessment Report within the agreed maximum period shall result in Kantara revoking the original Approval.

3.1.4.3 Permissable Exceptions

Applicants may request of the ARB a waiver from any of the above-expressed maxima and/or minima where that is supported by evidence of an over-riding condition and which is agreed-to by the Applicant's chosen Assessor. Such conditions might include, *inter alia*:

a) Requirements of the Assessor's auditing schema which permit or require such variance;

b) Conditions of another approval/certification scheme, or possibly regulatory or contractual obligation, to which the Applicant is subject mean that the Applicant would suffer an unreasonable cost- or efficiency-burden by undergoing two audits within a short space of time;

c) the Assessor believes that the Applicant requires greater time to gather sufficient evidence to sustain the PoT Assessment yet can justify an extended provisional Approval.

The ARB will examine closely any requests for waivers to ensure that a provisional Approval is not taken advantage off as a means to avoid the timely performance of a PoT Assessment required to underpin an Assessor's recommendation for full Approval.