Identity Assurance Framework: Rules governing Assurance Assessments

Version: 2.0

Date: 2015-09-04

Status: ARB policy

Approval: KIA20150831

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:

This document has been prepared by Participants of Kantara Initiative. Permission is hereby granted to use the document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact Kantara Initiative to determine whether an appropriate license for such use is available.

Implementation or use of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This Specification is provided "AS IS," and no Participant in the Kantara Initiative makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Implementers of this Specification are advised to review the Kantara Initiative's website (http://www.kantarainitiative.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Kantara Initiative Board of Trustees.

CONTENTS

I) INTRODUCTION

i.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.

i.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.

i.3 Changes in this revision

The principal reasons for changes in this revision are to:

a) revise the requirement concerning the performance of Period of Time assessments and when the 'operational period' is considered to commence;

b) more accurately title the 'Day Zero' assessment concept as 'Ready-to-Operate' assessments;

c) more clearly define what are the expectations upon Assessors when performing 'Ready-to-Operate' assessments, as opposed to 'Period-of-Time' assessments;

d) provide for the exclusion of criteria where the obligations they convey are transferred to the service's customers.

In addition, the opportunity has been taken to:

e) clarify that, whether Full or Component Service, the service must conform to ALL criteria in the CO-SAC (this is also stated in the SAC but is re-stated here

so as to reinforce that requirement);

f) neutralize the use of 'CSP' by replacing with plain language, given the chronic application of TLAs to describe electronic identity-related services in confusing and conflicting ways.

All revisions between v1.0 and v2.0 are shown with a grey background.

II) GLOSSARY

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

III) APPLICATION OF SERVICE ASSESSMENT CRITERIA

iii.1 Principles

Kantara's *Service Assessment Criteria* (SAC) 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.

iii.1.1 Statement of Conformity

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

a) "not within scope", where the criterion is excluded because the scope of the service does not include functionality which the criterion addresses;

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; or

d) "not applicable", with a justification as to why the criterion is deemed non-applicable when it otherwise falls within the scope (e.g. where a technical solution may permit a choice of means for conforming, those means not implemented would be 'not applicable').

Kantara prescribes the required minimum content of the SoC but not a specific structure. 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.

As stated in the SAC, all services must conform to all CO-SAC criteria. However, depending on whether the service in question is a Full or Component Service, how the criteria from the OP-SAC are addressed may vary, as described below.

iii.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 whose Provider 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].

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

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 as to the aggregate service, nor to any other non-Approved services.

iii.5.3 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 must address all 100% of the SAC OP-SAC criteria within the collective service. This assessment 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) 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;

b) 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;

c) 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.

Additionally, the Provider of a Full Service may exclude specific criteria where it can show that the responsibility for meeting those criteria is assumed by the Service Provider's customer(s). This provision allows for Providers' customers to efficiently leverage information and processes already in their hands. Providers who claim such exclusions must demonstrate how the excluded requirements are communicated to their customers and how their customers are obliged to fulfill

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.

them and the measures by which they shall be held accountable (typically through explicit notices and sections in service agreements).

Where a Provider seeks to exclude specific criteria by declaring them to be "not applicable" they must provide an explicit explanation of their purpose and intent, the affected criteria, and how the measures they will put in place to ensure the best likelihood of conformity being accomplished by the parties to whom those responsibilities are transferred.

iii.1.4 Initial Assessment versus Annual Conformity Review

Initial Assessments (i.e. those conducted for the purposes of a Grant of a three-year Approval) shall require assessment against all criteria defined in the Applicant's SoC and agreed-to by the ARB

The Kantara IAF's assessment model is based on established best practice as defined in ISO/IEC 17021, "*Conformity assessment - Requirements for bodies providing audit and certification of management systems*"), 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.

Therefore, the Annual Conformity Reviews performed on the first and second anniversaries of the initial Grant of Approval may have a reduced scope, as defined in the RAA.

iii.1.4.1 AL1 ACRs

For ACRs conducted at AL1, no actual assessment shall be required. CSP's shall submit to the ARB a self-assertion of their continued conformance with all applicable criteria (per their SoC).

iii.1.4.2 AL2, 3, 4 ACRs

For ACRs conducted at ALs 2, 3 and 4 the scope of criteria to be assessed shall be:

a) all criteria falling within the Core[3] set;

b) any criteria addressing areas of risk which are of concern to either the CSP itself or to its Assessor;

c) any criteria against which a non-conformity was identified and subsequently remediated (or for which remediation is outstanding) at the preceding assessment (of either type);

d) any criteria where there has been either:

   i) a change arising from a revision to the applicable version of the SAC; or

   ii) a significant change to how the service is operated and needs to be assessed (e.g. changes to outsourcing arrangements, or to applicable policies);

e) fifty per cent of all other criteria, such that, over the course of two ACRs, all

3 Those criteria considered to be Core and therefore requiring annual assessment are indicated as such in versions of the SAC issued after this document's release.

criteria not already included within a) – d) above are assessed.

For ACRs conducted at ALs 2, 3 and 4, CSP's shall submit to the ARB a KAR confirming continued conformance with all applicable criteria (per the CSP's SoC).

iii.1.5 Ready-to-Operate versus Period-of-Time Assessments

iii.1.5.1 Ready-to-Operate Assessments

It is a basic Kantara requirement that Approved services are fully operational. However, Service Providers may desire a Kantara Approval in advance of there being any operational history on which a Period-of-Time (PoT) assessment could be based. Kantara provides for such circumstances by accepting a Ready-to-Operate (RTO) 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) after the point in time at which operational records begin to be generated.

'Ready-to-Operate' shall be understood to require that the service meets all applicable criteria to the fullest extent practicable but for the provision of proof of effective operation through the furnishing as evidence of records accumulated during the service's operations. Other findings notwithstanding, no lesser readiness shall be accepted by Assessors as being sufficient to uphold a finding of conformance during a 'Ready-to-Operate' assessment. 'Nearly-Ready-to-Operate' is not a conformant state.

The availability of a RTO assessment is only open to providers of services at Assurance Levels 2, 3 and 4. All AL1 services shall be regarded as being operational by default and therefore be subject to a Period-of-Time audit.

Service Providers which elect to seek Approval based on a RTO 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 RTO Report, subject to the requirement that they must subsequently provide an Assessment Report based upon a PoT Assessment conformant to the operational period described below.

When Approval is granted on the basis of a RTO assessment the status of the Approval shall carry the qualifier 'Ready To Operate'.

iii.1.5.2 Period-of-Time Assessments

When the subject Service is already operational prior to being subjected to an Assessment, or becomes operational after previously undergoing a RTO assessment, the following periods of time are the minima 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 established logs and records of operations which can provide adequate supporting evidence):

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

Until such time as Approval is granted on the basis of a PoT Assessment, any 'Ready To Operate' Approval status based upon a RTO assessment will remain.

iii.16 Site visits

At AL2 and above, when performing either an 'initial' or 3-year re-approval assessment, Period of Time assessment, the Assessor shall conduct an on-site visit sufficient to ensure that operations are being adequately executed. Although site visits are not mandatory when an ACR is being performed, Assessors should consider, in their review of risk associated with the assessment, the need for an on-site visit and act accordingly.

No site visits are required at AL1.

IV) REVISION HISTORY

Vn.	Date	Status	Notes	Approved
1.0	2008-05-08	Initial Release	-	Liberty Alliance
2.0	2015-08-31	Public	Revision to eliminate un-used procedures, clarify/refine and reflect current practice, particularly regarding 'RTO' and 'PoT' assessment procedures.	Kantara ARB