

 Identity Assurance Framework:

Specification of a Service Subject to Assessment

**Version**: 5.0

**Publication Date** 2022-06-14

**Effective Date** 2022-10-01

**Status** ARB Policy

**Approval Authority** ARB

**Approval** 2022-06-13

**Contributors:** ARB members

**Abstract**

This document serves to describe a service being submitted to Kantara for Approval under its Trust Framework Operations Program, for both initial application and subsequently for formal Approval of the subject service. It is a *pro forma* intended to be presented in the Applicant’s house style as their own document.

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 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 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 Directors.

**IPR**: [Option Patent & Copyright: Reciprocal Royalty Free with Opt-Out to Reasonable And Non discriminatory (RAND)](https://kantarainitiative.org/confluence/x/DYBQAQ) | Copyright © 2022

Contents

[Notice 2](#_Toc95986125)

[1 INTRODUCTION 4](#_Toc95986126)

[1.1 Purpose 4](#_Toc95986127)

[1.2 Readership 4](#_Toc95986128)

[1.3 Overview & Preparation 5](#_Toc95986129)

[1.4 Changes in this revision 6](#_Toc95986130)

[2 PURPOSE & READERSHIP 7](#_Toc95986131)

[3 SERVICE DESCRIPTION 8](#_Toc95986132)

[3.1 Credential Service Provider 8](#_Toc95986133)

[3.2 Public Service Description 8](#_Toc95986134)

[3.3 Additional, Non-Public Service Description Details 9](#_Toc95986135)

[3.4 Service topology 9](#_Toc95986136)

[3.5 Service architecture 9](#_Toc95986137)

[4 EQUIVALENT CONFORMITY 10](#_Toc95986138)

[4.1 «Descriptive title» 10](#_Toc95986139)

[4.1.1 Description and justification 10](#_Toc95986140)

[4.1.2 Affected criteria 10](#_Toc95986141)

[4.1.3 Risk analysis 10](#_Toc95986142)

[4.1.4 Risk mitigation 11](#_Toc95986143)

[5 Criteria and Evidence 12](#_Toc95986144)

[5.1 Applicable Service Assessment Criteria 12](#_Toc95986145)

[5.2 Material changes 12](#_Toc95986146)

[5.3 Preceding Kantara Assessor Report 12](#_Toc95986147)

[6 Additional Information 13](#_Toc95986148)

# INTRODUCTION

Introductory note:

In this model Specification of a Service Subject to Assessment (hereafter simply the ‘S3A’) the sub-sections of the Introduction refer explicitly to this document.

In preparing their own specific instantiation of the model S3A, the Applicant should place in the Introduction their own text to explain their reasons for preparing the document and seeking Kantara Registered Service status and/or Approval, as required. They should also add any other introductory material they feel they require - **the following Kantara text within this section should then be deleted in its entirety**.

This S3A is applicable to Applicants for both a Component and a Full Service Application (refer to Kantara’s Service Approval Handbook, which is indispensable in the context of this S3A).

## Purpose

This document is intended for use by Credential Service Providers (CSP) for the production, as a prerequisite, of a Specification of a Service Subject to Assessment (S3A). Any CSP wishing to contract with a Kantara Accredited Assessor to conduct an Assessment for Kantara Service Approval or achieve Registered Service Status must submit an S3A. This is a required document for both Initial/Triennial Assessments and for Annual Conformity Reviews.

This document provides a high level overview to the CSP’s chosen Kantara Accredited Assessor, the Assurance Review Board, and to the Kantara Secretariat.

Conformance with this document is mandatory.

**CSPs adopting this pro forma to specify a particular service which is to be subjected to assessment should re-badge and re-designate this document as their own – once customized it is no longer a Kantara-owned or supported document and all Kantara-specific content / guidance should be removed.**

## Readership

This document is required reading for the following parties:

* **Kantara Accredited Assessors** who will be performing the Assessment of a Service, as defined by an S3A;
* **CSPs** submitting a Service (either a Component Service or a Full Service, where the selected Class of Approval permits) for an Assessment as the basis for seeking a Kantara Grant of Approval;
* **Kantara Initiative’s Assurance Review Board** who will use this document as the basis of Approving the CSPs application package;
* **Kantara Initiative’s representatives** who are available to offer guidance during the Assessment and Approval processes.

## Overview & Preparation

The document provides a framework of sections and sub-headings together with proposed standardized text. Authors of specific S3As are required to adopt the style, phrasing and terminology of this model to the fullest extent practical within the context of their own organizations. This will assist readers who have to deal with S3As from a number of different sources.

As previously stated, the Kantara Initiative [Service Approval Handbook](https://kantarainitiative.org/download/7590/) is required reading for S3A authors. It sets out explicit requirements for the Kantara Initiative Approval procedures and points to other detailed sources.

Within the suggested text there are a number of place-holders where authors should substitute the details of their own organizations and Services. These are indicated using « markers » as indicated in this sentence.

Throughout this document a distinction is made between an **Outline S3A** associated with an initial application for Registered Service status, and a **Comprehensive S3A,** which will become the driver for an actual Assessment (Initial / Triennial or an Annual Conformity Review).

Note: In the specific context of the S3A, the term ‘Full’ has no relationship as to whether the subject of the assessment is a ‘Full’ service or a service ‘Component’ – in either case, Outline and Comprehensive S3As are required, as further described below.

Kantara recognizes that the S3A is likely to be designated ‘Commercial In confidence’ and through the TMLA, Kantara undertakes to preserve the Applicant CSP’s confidentiality, except as qualified in certain Kantara documents, including this one. It is expected that the CSP will ensure that its confidentiality is protected by the terms of an independent agreement signed with its chosen Assessor.

As indicated above, certain parts of the Comprehensive S3A will be taken directly and used in preparing Kantara’s Grant of Approval. In order to alert the CSP as to which parts of their S3A will be extracted when preparing its Grant of Approval, those parts of this model document are framed in blue (as per this exemplar paragraph). Kantara reserves the right to put into the public domain information which the CSP provides in this context.

Kantara recommends that the contents of the S3A be agreed-to with the chosen Assessor prior to the Assessment. This will assist the Assessor in understanding the Service to be assessed and will ensure documentation of a sufficient and mutually-acceptable level of detail. It is furthermore a requirement that the S3A be revised as necessary to accurately define the Service as actually assessed.

Kantara recognizes that individual companies will have their own house styles and possibly specific service-related requirements that will dictate the final appearance of their S3A, and hence it is understood that the Kantara Initiativestyling of this model document may be substituted by the owner’s own style. It is further assumed therefore that any specific instantiation of this model will be subject to the owner’s own configuration management practices.

Improvements, enhancements and the provision of additional information to support the explanation of the SACs are fully encouraged within the constraint of following the model format as much as possible.

Definitions of terms and acronyms that are not defined in this document may be found in the Identity Assurance Framework [Glossary of Terms](https://kantarainitiative.org/download/iaf-1050-glossary-and-overview/).

Within the following Sections, an indication is given as to whether the heading and related text is applicable to an Outline S3A, a Comprehensive S3A or both.

## Changes in this revision

The principal reason for change in this revision are:

1. replaced and redefined §3.5 Assessor’s Service Definition as [§3.3](#_Additional,_Non-Public_Service) Additional, Non-Public Service Description Details;
2. clarified language to encourage comprehensive and precise responses from CSPs;
3. clearly defined the use of outline and comprehensive S3As; and
4. updated readers of the document to include the Assurance Review Board.

# PURPOSE & READERSHIP

The following text is suggested for those submitting an initial application, i.e. preparing an Outline S3A.

This document is the primary reference governing «organization»’s application for Kantara Registered Applicant status in respect of its «name of service» Service, as a «Full or Component» Service providing the credential services described herein at Assurance Level «state level(s)».

It provides the necessary high-level service description, target customer market, and outline technical specification required by the Kantara Initiative.

The document is intended to give:

1. «organization»’s management an understanding of what it is they are committing to;
2. the chosen Assessor, «assessor», an understanding of the scope of Assessment that «organization» requires to have conducted, and;
3. the KantaraAssurance Review Board the basis for considering and accepting «organization»’s application forRegistered Applicant status.

The following text is required for those wishing to have their services assessed and submitted for Kantara Approval, i.e. a Comprehensive S3A.

This document is the primary reference governing the Assessment and submission for Kantara Approval of «organization»’s «name of service» Service, as a «Full or Component» Service providing the credential services described herein at Assurance Level «state level(s)».

The document is intended to:

* + 1. give «organization»’s management an understanding of what it is they are committing to;
		2. define the full scope of the Assessment to be undertaken;
		3. define what evidence is to be provided and how it demonstrates compliance of the Service as a whole;
		4. form the central technical scoping of the contract between «organization» and its chosen Assessor, «assessor»;
		5. support «organization»’s submission to the Kantara Initiative Assurance Review Board and Executive Director for a Grant of Approval;

# SERVICE DESCRIPTION

The service provider must give a comprehensive and precise statement in each of the following sub-sections.

## Credential Service Provider

The following text is required in all S3As. In the case of an organization to which the terms used do not easily relate to its particular form of establishment and governance, please follow those guidelines in a manner which equivalently describes the nature of your organization.

This document relates to «organization», registered in «place of registration» under «registration reference / details» whose registered office is at «registered address». «organization» is «status, e.g. independent corporation / wholly owned subsidiary of etc.».

## Public Service Description

The following text is required in all S3As. CSPs should identify their service as being one of those described in the list of **service descriptors** which will be found at [Service Descriptors](https://kantarainitiative.org/trustoperations/classes-of-approval/#fourth), and use the applicable descriptor where required in the following description.

The Public Service Description will be used by Kantara when preparing the Grant of Approval. The provided text will be listed as the Scope of Approval on the Kantara [Trust Status List](https://kantarainitiative.org/trust-registry/trust-status-list/).

This S3A relates to «organization»’s service known as «name of service», which is submitted for Approval as a «insert applicable descriptor» under the following Classes of Approval:

«extract class of approval, assurance levels and any profile info from the Application for Service Approval (since this info is required by the Assessor who does not have access to the Application) »

«name of service» is a «Public Service Description of service».

For both Outline and Comprehensive S3As, address the following:

The Public Service Description will be preserved throughout the Assessment process, will be included in the Assurance Review Board Review and Assessment Report, and used subsequently by Kantara when preparing the Grant of Approval.

The Public Service Description should describe the principal features of the Service by setting out the purpose of the Service followed by additional detail, including, inter alia:

- features and functions incorporated;

- intended class(es) of users (subscribers and relying parties, as appropriate);

- list of tasks and usage;

- checks performed on supplied data;

- applicable restrictions;

- assumed user community characteristics;

- nature of provision / contracting with users & relying parties;

- etc.

This description must be a concise and accurate description of the scope and content of the SSA. It must be:

- suitable for unlimited public release;

- free of any jargon and marketing-hype;

- understandable to the non-specialist;

- suitable for prospective and actual customers of the service and for parties relying on the service;

- where the assessment includes the 63C\_SAC, the Applicant must include a unique identifier for the applicable Federation Agreement(s). Identifiers should preferably be machine parsable, (e.g. a uri, OID, …).

For a Comprehensive S3A, the Applicant must include a reference to the Service Definition, giving a specific version number or date of publication.

## Additional, Non-Public Service Description Details

Additional, non-public service details provide the Assessor and the Assurance Review Board with more comprehensive information about the Service than provided in the Public Service Description above. These details will assist in both the Assessment and the Assurance Review Board review. These Service Description details are not aimed at customers and are not publicly disseminated.

## Service topology

A system-level diagram (or diagrams) showing physical sites (geographic locations), where specific service components are located and what interconnectivity is employed should be provided. Supporting narrative shall be provided to describe the elements of the diagrams, plus indications of levels of redundancy and resilience that are built into the architecture, to explain the way in which the Service is managed and delivered.

## Service architecture

The level of detail provided should focus on details of the credential types issued and/or managed and applicable technologies, incorporated component services, and interfaces presented, such that the intended Assessor can plan the Assessment. It may also include specific descriptions of physical premises, hardware installations and software versions and configurations as may be relevant.

# EQUIVALENT CONFORMITY

If the Service Subject to Assessment includes features which the Applicant believes justify seeking Equivalent Conformity the following sub-section and all its parts should be included to describe each such instance. An equivalence might be described where the Applicant is unable to fulfill a Kantara SAC requirement but has an alternative means to mitigate the risk which the Kantara criterion addresses, employing an equivalent degree of rigour.

Alternatively, the Applicant may document such equivalent conformities separately and refer to them from within their Statement of Conformity (refer to KIAF-1340 Service Approval Handbook), in which case it is sufficient to list in this section the SAC, the criterion and the AL(s) for which equivalence is being claimed.

If the Applicant has no need to describe any Equivalent Conformity this section may simply state ‘None required’ (so as to preserve the section numbering system).

## «Descriptive title»

Apply a concise yet descriptive title to the specific equivalent conformity instance, capturing the functional nature of the service’s feature which requires a finding of equivalence, rather than referring to any specific criteria (this title may be used elsewhere as a label for this specific equivalence and needs to have a degree of uniqueness to aid in it being readily identifiable).

Note that this section needs to be repeated if multiple equivalent practices or controls are used for the assessed service, but one section can be used to meet several criteria.

### Description and justification

Provide a description of the aspects of the solution which differ from the ‘conventional’ approach, as might be implied by existing criteria, and justify why this provider or its service’s features require the move away from direct conformity into needing to show an equivalent solution.

Given that [§3.3 above](#Section3) provides a detailed description it may be sufficient to rely upon that as the source of description (ensuring that it can be captured discretely, rather than as an integral part of the description of the whole, e.g. having a discrete reference) and simply provide the justification here.

Bear in mind that higher Assurance Levels must be justified by a greater degree of rigor, consistent with demonstrating conformity with any other criteria at the selected Assurance Level.

### Affected criteria

Identify, for each SAC and for each AL at which the service is being assessed, the criteria within the SAC against which this specific equivalent solution is to be assessed.

### Risk analysis

Identify the risks inherent in the service if it does NOT fulfill the original criteria (i.e. determine the objectives of the existing criteria and what they were attempting to protect against or achieve).

### Risk mitigation

Provide a risk assessment which demonstrates adequate mitigation of risks identified in §4.1.3 above such that the equivalence is evident. Show how the proposed alternative conformity addresses the risk(s) which the original criterion sought to mitigate and achieves equivalent rigour in its mitigation of those risks. Where there is a standards-based approach which is: a) a part of the original criteria from which divergence is being justified; and/or, b) which underpins the justification for adopting an equivalent solution; reference to the applicable standard(s) should be made to ensure clarity.

As an alternative to the above three discrete clauses, and depending on how the Applicant chooses to present the required information, a single clause “§4.1.2 Affected criteria, risk analysis and mitigation” may be used so long as the scope and purpose of the three individual sections proposed above as §4.1.2 to §4.1.4 are fulfilled .

# Criteria and Evidence

## Applicable Service Assessment Criteria

This should state the Class of Approval and the included SAC suite, in addition to which a Statement of Applicable Criteria (see KIAF-1340 Service Approval Handbook) covering each of the SACs within the assessment must be presented as a separate document.

In an Outline S3A there is no need to cite the SAC version, since the actual version used will be determined according to that current at the time the Assessment is undertaken.

«organization»’s «name of service» is submitted for Assessment against «state titles of each SAC used as reference for this Application» version «state version of each SAC used as reference for this Application», with the criteria applicability as stated in «reference to SoCA».

## Material changes

Unless the assessment in question is an Initial Assessment, state any material changes since the last assessment. Such considerations should include, inter alia: ownership; jurisdiction; applicable legislation; policies; processes and procedures; management structure; physical location(s); system architectural / technical configurations; external parties; other assessment / audit / certification findings.

If there have been none, state so.

## Preceding Kantara Assessor Report

Where such exists, insert a reference to the most recent KAR and include a copy with the related S3A in the evidence provided to the Assessor. This allows the Assessor to ensure that any previous non-conformities have been adequately resolved.

# Additional Information

The Applicant may provide whatever additional information is felt necessary or useful to support the S3A, whether an Outline S3A or a Comprehensive S3A, e.g. any specific national government requirements required to be fulfilled in addition to those established by Kantara.

The Applicant may include additional requirements that take the Assessment beyond the scope of the Kantara Approval. It is recommended that the necessary additional parts of the document be placed in the most appropriate section (e.g. additional criteria against which to be assessed might go under §5.1, with the proposed evidence under §5.2).

Annexes may also be added where required.

Applicants should ensure that any additional information is clearly included as such, rather than as Kantara-specific information.

This section may be omitted when no additional information need be provided.