Identity Assurance Framework: Specification of a Service Subject to Assessment

Version: 2.3

Date: 2014-07-16

Editor: Richard G. Wilsher
Zygma LLC

Contributors

The full list of contributors can be referenced here:
http://kantarainitiative.org/confluence/display/idassurance/IAF+2.0+Contributors

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 is comprised of a set of documents that 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 the *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 present document sets out the required structure of a Specification of a Service subject to Assessment, a primary component of an Application for Kantara Approval and the Assessment required to support that Application.

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

Filename: Kantara IAF-3520 S3A v2-3

Notice

Contents

1 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's own text to explain their reasons for preparing the document and seeking Kantara Registered Applicant status and/or Approval, as required, should be placed in the Introduction. They should also add any other introductory material they feel they require and the following Kantara text within this section should be deleted in its entirety.

This S3A is applicable to Applicants for both a Component and a Full Service Application (refer to Kantara's Rules governing Assurance Assessments).

1.1 Purpose

This document is intended for use by Credential Service Providers (CSPs) 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 Applicant Status must submit an S3A.

This document provides a high level overview to the CSP's chosen Kantara Accredited Assessor and to the Kantara Secretariat.

Conformance with this document is mandatory.

1.2 Readership

This document is required reading for the following parties:

- **Kantara Accredited Assessors** who will be performing the Assessment of a Credential Service Provider, as defined by an S3A;
- **CSPs** submitting a Service (either a Component Service or a Full Service) for an Assessment as the basis for seeking a Kantara Grant of Approval;
- **Kantara Initiative's representatives** who are available to offer guidance during the Assessment and Approval processes.

1.3 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 Assurance Assessment Scheme 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 a request for Registered Applicant status, and a **Full S3A,** which will become the focus of the Assessment itself.

Note: 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 Full S3As are required, as further described below.

Only the Outline S3A should be submitted to Kantara. The Full S3A is likely to be designated 'Commercial In confidence'. Confidentiality is protected by the terms of an independent agreement signed with the chosen Assessor. However, certain parts of the Full S3A will be taken directly and used in preparing the Kantara Assessment Report and ultimately in Kantara's Grant of Approval.

In order to alert the CSP as to which parts of their S3A will be extracted when preparing their Kantara Assessment Report, those parts of this model document are framed in blue (as per this exemplar paragraph). Kantara will extract such text from the Kantara Assessment Report and use it when preparing its Grant of Approval.

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 Initiative styling 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.

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

1.4 Changes in this revision

The principal reason for changes in this revision is the introduction of a new section in which Applicants can describe and justify any Comparability solutions their service may provide. All changes in this revision are indicated by grey shading.

2 PURPOSE & READERSHIP

The following text is suggested for those seeking Kantara Registered Applicant status, i.e. preparing an Outline S3A.

This document is the primary reference governing «company»'s application for Kantara Registered Applicant status in respect of its «name of service» Service, as a [Full | Component «delete as applicable»] 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:

i) «company»'s management an understanding of what it is they are committing to;

ii) the chosen Assessor, «assessor», an understanding of the scope of Assessment that «company» requires to have conducted, and;

iii) the Kantara Assurance Review Board the basis for considering and accepting «company»'s application for Registered Applicant status.

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

This document is the primary reference governing the Assessment and submission for Kantara Approval of «company»'s «name of service» Service.

The document is intended to:

i) give «company»'s management an understanding of what it is they are committing to;

ii) define the full scope of the Assessment to be undertaken;

iii) define what evidence is to be provided and how it demonstrates compliance of the Service as a whole;

iv) form the central technical scoping of the contract between «company» and its chosen Assessor, «assessor»;

v) support «company»'s submission to the Kantara Initiative Board of Trustees for a Grant of Approval;

3 SERVICE DESCRIPTION

3.1 Credential Service Provider

The following text is required in all S3As.

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

«company»'s additional contact details are as follows: Contact person for the purposes of this Assessment: Primary contact:

«name, title»
«address»
«telephone»
«email»

Secondary contact:

«name, title»
«address»
«telephone»
«email»

*The following **additional** text is suggested for those wishing to have their services assessed and submitted for Kantara Service Approval (i.e. Full S3A). **If all following contacts are already identified in the ASA then simply state so, else add additional contacts here**.*

Contact points with regard to the service (e.g. Customer Support etc):

Contact 1:

«functional title»
«address»
«telephone»
«email»
«url»

Contact 2:

«functional title»
«address»
«telephone»
«email»
«url»

«.... additional contacts as desired»

3.2 Public Service Description

The following text is required in all S3As

This S3A relates to «company»'s service known as «name of service».

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

The Public Service Description will be preserved throughout the Assessment process, will be included in the 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;*

.

Additionally, for a Full S3A, the Applicant must include a reference to the Service Definition , giving a specific version number or date of publication

3.3 Service topology

For those seeking Kantara Registered Applicant status (i.e. Outline S3A), 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. Brief supporting narrative should be provided to describe the elements of the diagram(s).

For an Assessor's Service Definition (i.e. Full S3A), 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 should be provided to describe the elements of the diagrams to a further level of detail, 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 .

3.4 Service platform

In an Outline S3A the level of detail provided under this heading need only be a generalized description.

For a Full S3A, the level of detail provided should include specific descriptions of physical premises, hardware installations and software versions and configurations, plus details of the credential types issued and/or managed and applicable technologies, such that the intended Assessor can plan the Assessment.

3.5 Assessor's Service Definition

This section is only required in a Full S3A. *It must give a comprehensive and precise definition of the Service, its constituent parts and its internal functions, suitable for Kantara-Accredited Assessors to identify and scope the Service for the purpose of the Assessment. It must provide information beyond the extent of that which would be found in the Service (Certification) Policy, Service Practice Statement and Service Policy Disclosure Statement which an assessor would need to know in order to effectively conduct the Assessment. The Assessor's Service Definition is not aimed at customers and is not required to be publicly disseminated.*

This definition may be in a separate document but it is defined in this Model S3A, and should consist of an extension to the detail given in the Outline S3A, in §3.2 to §3.4 inclusive.

4 COMPARABLE CONFORMITY

If the Service Subject to Assessment includes features which the Applicant believes justify seeking Comparable Conformity the following sub-section and all its parts should be included to describe each such instance.

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

4.1 «Descriptive title»

Apply a concise yet descriptive title to the specific comparable conformity instance, capturing the functional nature of the service's feature which requires a finding of comparability, rather than referring to any specific criteria (this title may be used elsewhere as a label for this specific comparability 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 comparable controls are used for the assessed service, but one section can be used to meet several criteria.

4.1.1 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 a comparable solution. Given that §3.5 above 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.

4.1.2 Affected criteria

Identify, for each AL at which the service is being assessed, the criteria within the SAC against which this specific comparable solution is to be assessed. Refer to the SAC part (e.g. 'CO_SAC) as well as the individual criterion tag(s).

4.1.3 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).

4.1.4 Risk mitigation

Provide a risk assessment which demonstrates adequate mitigation of risks identified in §4.1.3 above such that the comparability is evident. 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 a comparative 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 in conjunction with a table having three columns bearing the discrete title of the three individual sections proposed above as §4.1.2 to §4.1.4, the contents of which fulfil the above-stated requirements.

5 CRITERIA AND EVIDENCE

5.1 Applicable Service Assessment Criteria

In an Outline S3A this section may simply be declared as 'TBD', since the actual version used will be determined according to that current at the time the Assessment is undertaken.

«company»'s «name of service» is submitted for Assessment against "*Kantara IAF-1400 Service Assessment Criteria"* version «state version of SAC used as reference for this Application».

5.2 Statement of Conformity

The SoC may be included here, be a separate document or be included within another document. However, it is mandatory to provide it to Kantara in a form which allows the Kantara Secretariat to determine the scope of coverage of the OP-SAC. Tables provided in the SAC are recommended as the basis for the SoC and allow for i) the specification of the criterion tag; ii) how the criterion is fulfilled, and iii) the source(s) of evidence.

For a Full S3A, the chosen Assessor must be provided with all three pieces of information, per criterion. In an Outline S3A this section may simply state how it is proposed to fulfill the OP-SAC criteria, i.e. items i) and ii) from above: for a Component Service this will be less than 100% of the OP-SAC criteria; for a Full Service this will address all OP-SAC criteria and indicate whether, per criterion, conformity will be accomplished by the Applicant Service Provider or by a previously-Approved Component Service..

Criteria which are subject to assessment based upon comparability (see §4 above) should be clearly identified as such within the SoC, for both an Outline and Full S3A.

6 ADDITIONAL INFORMATION

The Applicant may provide whatever additional information is felt necessary or useful to support the S3A, whether an Outline S3A or a Full 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, and may be an alternative holding place for the SoC.

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.