The Road to Multilateral Recognition of Identity Assurance Programs

A Comparison of Kantara Initiative Requirements

Editor: KENNETH DAGG

Contributors:

Howard Staple	Identity & Information Assurance Advisor, Identity Assurance Programme, Government Digital Services, Cabinet Office
Alastair Treharne	Identity Assurance Advisor, Identity Assurance Programme, Government Digital Services, Cabinet Office
Joni Brennan	Executive Director, Kantara Initiative

Abstract:

This study is one of a set of reports prepared by the Kantara Initiative to assess if it is viable for the United Kingdom (UK) Cabinet Office to recognize Identity Providers approved by other international bodies for use in the UK. In other words, the purpose of the series of studies is to determine the viability of multilateral recognition of national identity assurance programs.

This specific report presents, based upon a high level analysis, observations from a comparison of Kantara Initiative's requirements with the requirements specified by the UK. It also recommends activities for additional analysis to determine if Kantara Initiative requirements fully meet the specific requirements that the UK has established.

Contents

1 PROJECT OVERVIEW

1.1 Project Purpose

This project is being undertaken by the Kantara Initiative to assess the processes currently being used by other international bodies to accredit and certify/approve Identity Providers (IDAs) with the goal of determining if it is viable for the United Kingdom (UK) Cabinet Office to recognize these IDAs for use in the UK. In other words, the purpose of the series of studies is to determine the viability of multilateral recognition of national identity assurance programs.

To test the feasibility of this approach of the UK Cabinet Office and start down the road to multilateral recognition, this project will provide a high level assessment of the processes used by Kantara Initiative to accredit and approve IDAs for use by the Government of the United States of America (US).

It should be noted that for legal and insurance reasons, Kantara Initiative "approves" rather than "certifies" IDAs. When in the context of Kantara Initiative the term "approve" will be used while in the context of the UK the term "certify" will be used.

1.2 Project Business Objectives

This project will specifically identify options, recommendations and timeframes based upon an:

- Assessment of the equivalence of Kantara Initiative's IAF requirements against the UK's requirements for Certification Bodies (CBs) and IDAs.
- Assessment of the equivalence of US Government and Cabinet Office requirements for CBs and IDAs including authentication governance.
- Assessment of the future direction and evolution of the National Institute of Standards and Technology (NIST) Electronic Authentication Guideline (Special Publication 800-63).

The options, recommendations and timeframes identified in this assessment will contribute to the Cabinet Office of the UK Government recognizing other jurisdictions as Accredited CBs that are able to certify IDAs to Cabinet Office standards, so that the Cabinet Office does not have to carry out the assessment of the IDAs. This in turn contributes to the Cabinet Office realizing its vision to create a market of certified, customer-focused services in the private sector that will provide a consistent way for customers to access any public service, and potentially private sector services.

2 Contents

Section 3 of this document presents, based upon a high level analysis, observations from a comparison of Kantara Initiative's requirements with the requirements specified by the UK. Section 3 also recommends activities that could be undertaken to undertake additional analysis to determine if Kantara Initiative requirements fully meet the requirements that the UK has established.

Section 4 identifies requirements contained in the Kantara Initiative IAF that the UK might want to consider for its Good Practice Guides (GPGs).

Section 5 summaries the findings from the comparison of Kantara Initiative's requirements with the requirements specified by the UK.

Appendix A contains a list of the Acronyms, Abbreviations and terms used in the document. Appendix B identifies the materials that were analyzed. Appendix C contains more details on the findings of the analysis.

3 Requirements Comparison

This section presents, based upon a high level analysis, the observations and recommendations from a comparison of Kantara Initiative's requirements with the requirements specified by the UK in the following documents:

- GPG 43: Requirements for Secure Delivery of Online Public Services (RSDOPS) - Issue No: 1.1
- GPG 44: Authentication Credentials in Support of HMG Online Services – Issue No: 2.0, and
- GPG 45: Validating and Verifying the Identity of an Individual in Support of HMG Online Services - Issue No: 2.3
- GPG 53: Transaction Monitoring for HMG Online Service Providers, Issue No: 1.0
- Specification for Organisations Providing Proofing and Authentication of Digital Identities, v0.3 Draft
- Specification for Certification Bodies Certifying Identity Assurance Providers, Draft
- IPV (Identity Proofing and Verification) Operations Manual, version 2.3.1
- Identity Assurance Hub Service SAML 2.0 Profile, version 1.1a

The following documents (Kantara Initiative's Identity Assurance Framework (IAF)) contain the requirements used by Kantara Initiative to assess IDAs:

- Kantara IAF-1200 Levels of Assurance v2-0
- Kantara IAF-1300 Assurance Assessment Scheme v3-0
- Kantara IAF-1400 Service Assessment Criteria v4-0
- Kantara IAF-1600 Assessor Qualifications and Requirements v2-0
- Kantara IAF-1800 Rules governing Assurance Assessments v1-0

Appendix C contains details of the high-level assessment.

It also recommends additional analysis activities to determine if Kantara Initiative requirements fully meet some very specific requirements established by the UK.

3.1 GPG 43

Levels of Assurance

Observations

Kantara Initiative's approach, while seeming to examine different aspects of the situation, covers essentially the same overall aspects as the UK's analysis with the exception of explicitly examining privacy. The aspects examined by Kantara Initiative implicitly include privacy (i.e., unauthorized release of sensitive information and Inconvenience, distress, or damage to standing or reputation) but a risk analysis process or a risk analyst could, if not privacy aware, could overlook this aspect. The result of both

risk analyses is that Service Providers identify the level of assurance they require for the electronic transaction system.

Kantara Initiative does not explicitly include privacy as one of the aspects to be examined when determining the impact of Identity Authentication Errors.

Recommendations

If the difference in numeric tags is a perceived issue the UK could change its numbering scheme. This recommendation is made (rather than Kantara Initiative changing its numbering scheme) as many other jurisdictions have already adopted the 1 to 4 designation scheme.

3.2 GPG 44

3.2.1 AC Element A: Credential Type

Observations

Kantara Initiative has similar Service Assessment Criteria

3.2.2 AC Element B: Quality of the Credential

Observations

Kantara Initiative does not have equivalent Service Assessment Criteria. Specifically, Kantara Initiative does not have:

- service assessment criteria at any of the LOA levels to assess for specific measures to prevent prediction or duplication.
- criterion in LOA level 2 that require software cryptographic tokens to be in accordance with FIPS 140-2 Level 1 to be Level 1 or higher.

3.2.3 AC Element C: Management of the Credential

Observations

While Kantara Initiative has some equivalent Service Assessment Criteria it does not have some requirements. Specifically, Kantara Initiative does not have:

- service assessment criteria in LOA level 2 that request that the Authentication Provider:
  - Be able to suspend a Credential immediately from the primary system that manages credentials.
  - Be able to permanently revoke a Credential with immediate effect.

    - Ensures that the Credential is under the control of the person/user to whom it belongs before, or on, first use.
- service assessment criteria in LOA level 3 and 4 that request that the Authentication Provider has taken sufficient measures to ensure that the Credential can reasonably be assumed to have been delivered into the possession of the person to whom it belongs.

3.2.4 AC Element D: Monitoring

Observations

While Kantara Initiative has equivalent Service Assessment Criteria for most UK requirements it does not have some requirements. Specifically, Kantara Initiative does not have service assessment criteria in LOA level 3 and level 4 that ensure transaction monitoring and analysis take place to detect and report abnormal authentication behaviour.

3.2.5 AC Element E: Authentication Service Characteristics

Observations

While Kantara Initiative has equivalent Service Assessment Criteria for most UK requirements it does not have some requirements. Specifically, Kantara Initiative does not have:

- service assessment criteria in LOA level 3 and 4 that check for measures that are effective at preventing use by non-human operators.
- service assessment criteria in LOA level 3 and 4 that check for measures that protect the Credential from compromise, even if the communication channel is compromised.

3.2.6 AC Element F: Information Assurance Maturity of the Authentication Provider

Observations

While Kantara Initiative has equivalent Service Assessment Criteria for some UK requirements it does not have the majority of the requirements. Specifically, Kantara Initiative does not have:

- service assessment criteria in LOA level 2 that check that all systems supporting the use of the Credential have a consistent time.
- service assessment criteria in LOA level 2 that check that an Authentication Provider has a records management system for identifying, classifying, prioritising,

storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential.

- service assessment criteria in LOA level 3 that check that all systems supporting the use of the Credential have a consistent time using a Good Industry Practice time source.
- service assessment criteria in LOA level 4 concerning information security management system that specify that it should be independently certified.
- service assessment criteria in LOA level 4 concerning information security management system that explicitly identify that it should include an independently certified audit regime.
- service assessment criteria in LOA level 4 concerning information security management system that explicitly identify that it should include an independently certified records management system.
- service assessment criteria in LOA level 4 that check that all systems supporting the use of the Credential have a consistent time using a trusted Industry Practice time source such as Stratum 1 (or equivalent).

Recommendations

Kantara Initiative considers:

- adding an example to the service assessment criteria in LOA level 2 that check that an Authentication Provider applies controls during system development, procurement, installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications to specifically mention a monitoring regime that detects unexpected and undesirable activity within the service.
- adding an example to the service assessment criteria in LOA level 2 that check that an Authentication Provider demonstrates a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community to specifically mention the conduct of regular risk assessments and the handling of exceptions.
- modifying the service assessment criteria in LOA level 3 and level 4 concerning Internal Service Audit to Service Audit. Additionally, the description should include provision of either a first-party audit or an independent audit at least once every 12 months. The description of the service assessment criteria should also make mention of a forensic readiness plan.
- adding an example to the service assessment criteria in LOA level 3 that check that an Authentication Provider to demonstrate that it applies controls during system development, procurement, installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications to specifically mention a monitoring regime that detects unexpected activity within the service and includes a schedule of independent vulnerability and penetration tests.
- adding an example to the service assessment criteria in LOA level 3 that check that an Authentication Provider provides physical and logical access control to

specifically mention an independently audited internal monitoring regime that detects unusual, or malicious, activity of the Authentication Provider's staff and others as well as the inclusion of a schedule of independent vulnerability and penetration tests.

3.3 GPG 45

3.3.1 IPV Element A – Strength of Identity Evidence

Observations

While Kantara Initiative has equivalent Service Assessment Criteria for some UK requirements it does not have the majority of the requirements. Specifically, Kantara Initiative:

- service assessment criteria at LOA level 1 In-Person Public Identity Proofing specify self-assertion of identity and self-attestation of evidence instead of the examination, but not validation or verification, of identity evidence and that the Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates or a photograph / image / Biometric of the person to whom it relates.
- service assessment criteria at LOA level 4 In-Person Public Identity Proofing do not include a requirement that issued Identity Evidence contains a Biometric of the person to whom it relates.

UK requirements do not separate "In-Person Public Identity Verification"; "Remote Public Identity Verification"; "Current Relationship Identity Verification"; and "Affiliation Identity Verification".

Recommendations

Additional analysis is required to determine if the identity proofing activities required by Kantara Initiative to meet LOA level 3 and 4 requirements satisfy UK Money Laundering Regulations 2007.

3.3.2 IPV Element B – Outcome of the Validation of Identity Evidence

Observations

Kantara Initiative specifies mechanisms to verify information provided by the applicant depending on the information that has been provided for a specific LOA level.

Recommendations

Additional analysis, beyond the scope of this study, is required to analyze whether the mechanisms specified by Kantara Initiative to validate information provided by the applicant at each LOA level fully meet the requirements identified in GPG 45.

3.3.3 IPV Element C – Outcome of Identity Verification

Observations

Kantara Initiative provides mechanisms to verify information provided by the applicant depending on the information that has been provided for a specific LOA level.

Recommendations

Additional analysis, beyond the scope of this study, is required to analyze whether the mechanisms specified by Kantara Initiative to verify information provided by the applicant at each LOA level fully meet the requirements identified in GPG 45.

3.3.4 IPV Element D – Outcome of Counter-Fraud Checks

Observations

Kantara Initiative does not explicitly undertake Counter-Fraud Checks for any LOA level.

Recommendations

Additional analysis, beyond the scope of this study, is required to determine how Counter-Fraud Checks can be added to the service assessment criteria at each LOA level in order to satisfy the requirements identified in GPG 45.

3.3.5 IPV Element E – Activity History of the Claimed Identity

Observations

Kantara Initiative does not explicitly undertake checks of activity history for any LOA level.

Recommendations

Additional analysis, beyond the scope of this study, is required to determine how Activity History of the Claimed Identity can be added to the service assessment criteria at each LOA level in order to satisfy the requirements identified in GPG 45.

3.4 Service Delivery Requirements

Observations

Kantara Initiative service assessment criteria address some, but not all, of the requirements specified by the UK. Specifically, Kantara Initiative does not have service assessment criteria to address the requirements for Service Delivery identified by the UK.

Recommendations

Kantara Initiative implements service assessment criteria to address the requirements for Service Delivery identified by the UK.

3.5 Specification for Organisations Providing Proofing and Authentication of Digital Identities

Observations

While Kantara Initiative has equivalent Service Assessment Criteria for most UK requirements it does not have all of the requirements. Specifically, Kantara Initiative does not have:

- service assessment criteria to ensure that an organization that has been suspended by one Certification Body, due to a failure to implement the requirement in this specification, is not allowed to practice for any other Certification Body until that suspension is revoked and the requirements are met.
- service assessment criteria to ensure that an organization agrees to their current or past Certification Body sharing information with other Certification Bodies and other relevant third parties where appropriate.
- service assessment criteria to ensure that at least five per cent of Identities proofed are internally audited within a 12-month period.
- service assessment criteria to ensure that an organization is required to identify and systematically examine the cause and consequences of any issues raised during internal audits and document the findings.
- service assessment criteria to ensure that an organization is required to carry out corrective actions including rectification of the particular occurrence(s) identified during internal audits and initiate measures to prevent recurrence.
- service assessment criteria to ensure that an organization is required to have in place and operate a documented complaints procedure.
- service assessment criteria to ensure that an organization is required to have a documented process to define how and what they will report to the IDA service or other Organisations, security incidents and suspect fraudulent activity that they detects in relation to the IDA Service.

Recommendations

Kantara Initiative should create a profile for the UK that specifies that the indemnity should cover of at least six years is provided for any identities proofed or authenticated.

3.6 Specification for Certification Bodies Certifying Identity Assurance Providers

Observations

Kantara Initiative's Assurance Assessment Scheme potentially meets the requirements of BS EN ISO/IEC 17065.

Recommendations

Further investigation by personnel expert in BS EN ISO/IEC 17065 will need to be undertaken to confirm this preliminary finding concerning Kantara Initiative's Assurance Assessment Scheme, Assessor Qualifications & Requirements and Rules governing Assurance Assessments.

4 Potential Modifications to GPG 44 Requirements

Kantara Initiative Service Assessment Criteria include the following requirements that the UK might want to consider for GPG 44:

1. GPG 44 has the requirement that the issuing process for a Credential should take all reasonable measures to ensure it has been delivered into the possession of the person to whom it belongs. Kantara Initiative extends that requirement to require Subscribers and Subjects to:
   - indicate, prior to receiving service, that they have read and accept the terms of service as defined in the Service Definition;
   - at periodic intervals, determined by significant service provision events (e.g. issuance, re-issuance, renewal), re-affirm their understanding and observance of the terms of service; and
   - always provide full and correct responses to requests for information.

   In addition, Kantara Initiative requires that the IDA obtain and maintain a record (hard-copy or electronic) of the acceptance.
2. Kantara Initiative has different service assessment criteria according to the following types of identity proofing:
   - In-Person Public Identity Verification
   - Remote Public Identity Verification
   - Current Relationship Identity Verification
   - Affiliation Identity Verification
   - Verification of an existing recognized credential
3. Kantara Initiative allows revocation of a credential by someone other than the IDA (i.e., the Subscriber) upon the requestor and the nature of the request being verified as rigorously as the original identity proofing.

5 Conclusions

A high-level analysis of Kantara Initiative IAF requirements indicates that Kantara Initiative has equivalent requirements to the majority of the requirements established by the UK. The requirements that Kantara Initiative does not have could be addressed by either evolving the IAF or by creating a profile for the UK that includes those requirements. There are several cases where further analysis of Kantara Initiative requirements must be undertaken to ensure that they meet jurisdictional specific requirements that have been established by the UK.

The high-level analysis also identified several requirements contained in the Kantara Initiative IAF that the UK might want to consider for inclusion in their requirements.

While the processes used by both Kantara Initiative and the UK appear to be similar further investigation is required by experts in that process to validate that they are equivalent. This could be accomplished by either undertaking further analysis or by having Kantara Initiative have its process certified by the American National Standards Institute (ANSI) as meeting the specifications of ISO/IEC 17065.

APPENDIX A – ACRONYMS, ABBREVIATIONS AND GLOSSARY

This appendix expands acronyms and abbreviations used in this document.

Term	Definition
ANSI	American National Standards Institute
CB	Certification Body
CESG	Communications-Electronics Security Group
FIPS	Federal Information Processing Standards
GPG	Good Practice Guide
HMG	Her Majesties Government
IAF	Identity Assurance Framework
ICT	Information and Communications Technology
IDA	Identity Assurance Provider
IPV	Identity Proofing and Verification
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization and the International Electrotechnical Commission
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
RSDOPS	Requirements for Secure Delivery of Online Public Services
TLS	Transport Layer Security
UK	United Kingdom
UKAS	United Kingdom Accreditation Service
US	United States of America

APPENDIX B – ANALYSIS REFERENCE MATERIAL

- Good Practice Guide 43 - Requirements for Secure Delivery of Online Public Services, Issue No: 1.1, December 2012, Communications-Electronics Security Group (CESG), Crown copyright 2012.
- Good Practice Guide No. 44 - Authentication and Credentials for use with HMG Online Services, Issue No: 2.0, October 2014, CESG, Crown copyright 2014
- Good Practice Guide No. 45 - Identity Proofing and Verification of an Individual, Issue No: 2.3, July 2014, CESG, Crown copyright 2014
- Good Practice Guide No. 53 - Transaction Monitoring for HMG Online Service Providers, Issue No: 1.0, April 2013, CESG, Crown Copyright 2013
- Specification for Organisations Providing Proofing and Authentication of Digital Identities, v0.3 Draft, Date: Unknown
- Specification for Certification Bodies Certifying Identity Assurance Providers, Draft, Date: Unknown
- IPV (Identity Proofing and Verification) Operations Manual, version 2.3.1, December 4, 2014
- Identity Assurance Hub Service SAML 2.0 Profile, version 1.1a, September 11, 2013, Identity Assurance Programme, Crown Copyright 2013
- Identity Assurance Framework-1000: Overview, Version 2.0, April 4, 2010, Kantara Initiative Copyright 2010
- Identity Assurance Framework-1200: Assurance Levels, Version 2.0, April 4, 2010, Kantara Initiative Copyright 2010
- Identity Assurance Framework-1300: Assurance Assessment Scheme, Version 3.0, February 7, 2013, Kantara Initiative Copyright 2013
- Identity Assurance Framework: Service Assessment Criteria-1400, Version 4.0, May 12, 2014, Kantara Initiative Copyright 2014
- Identity Assurance Framework-1600: Assessor Qualifications & Requirements, Version 2.0, April 24, 2010, Kantara Initiative Copyright 2010
- Identity Assurance Framework-1800: Rules governing Assurance Assessments, Version 1.0, February 7, 2013, Kantara Initiative Copyright 2013

APPENDIX C – SPECIFIC ANALYSIS OF REQUIREMENTS

This appendix provides further high-level observations concerning the comparison of Kantara Initiative requirements to UK requirements.

Compliance with Service Delivery Requirements

Service Delivery Requirements	Observations about Kantara Initiative
Requirements that a provider must meet in order to be operational are identified in the following areas: • Service Readiness Assessment Criteria • Service Reporting • Service Management Information • ICT Release and Deployment Management • IDA Onboarding • Configuration and Configuration Management • Incident and Problem Management • Service Desk • User Experience	Kantara Initiative service assessment criteria address some, but not all, of the requirements specified by the UK. Information Security Management Criteria address the way in which the enterprise manages the security of its business, the specified service, and information it holds relating to its user community. It includes service assessment criteria that address, for each LOA level, the following: • Documented policies and procedures • Policy Management and Responsibility • Risk Management • Continuity of Operations Plan • Configuration Management • Quality Management • System Installation and Operation Controls • Internal Service Audit • Audit Records • Best Practice Security Management Operational Infrastructure criteria address the infrastructure within which the delivery of the specified service takes place. It puts particular emphasis upon the personnel involved, and their selection, training, and duties. It includes service assessment criteria that address, for each LOA level, the following:

	• Technical security • Defined security roles • Personnel recruitment • Personnel skills • Adequacy of Personnel resources • Physical access control • Logical access control

OBSERVATION: Kantara Initiative does not have service assessment criteria to address the requirements for Service Delivery identified by the UK.

GPG 43 Compliance – Levels of Assurance

GPG 43 states that a Service Provider should undertake a risk analysis that considers threats, vulnerabilities and service or transaction value as well as the expectations of the stakeholders. Based on the results of the risk analysis, an understanding of the budgets, capabilities, motivations, and risk tolerances of the organisation, and an understanding of the direct and indirect consequences of a failure of each security component, a security profile is developed that specifies a level for each of the following security components:

- End User
  - Personal Registration
  - Corporate Registration
  - Authentication
  - Authorisation
  - Privacy
- Server
  - Information Access
  - Information Availability
- Network
  - Communications Security
  - Network Authentication
  - Network protection
  - Situational awareness
- Business logic
  - Internal accountability
  - External accountability
- Assurance
  - Organisational assurance

- Technical assurance

Kantara Initiative advocates that a risk assessment be undertaken for each electronic transaction system to determine if the impact of Identity Authentication Errors on the following factors is Minimum, Moderate, Substantial or High:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to govt. agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

Kantara Initiative's approach, while seeming to examine different aspects of the situation, covers essentially the same overall aspects as the UK's analysis with the exception of explicitly examining privacy. The aspects examined by Kantara Initiative implicitly include privacy (i.e., unauthorized release of sensitive information and Inconvenience, distress, or damage to standing or reputation) but a risk analysis process or a risk analyst could, if not privacy aware, could overlook this aspect.

The result of both risk analyses is that Service Providers identify the level of assurance they require for the electronic transaction system.

The meaning of the increase in level of assurance (i.e., from level 1 to level 2) means in essence the same for both Kantara Initiative and the UK: as levels of risk to a service or transaction increase then what needs to be done from a security and assurance perspective increases in proportion.

The following table provides an overview description of the confidence an electronic transaction service requires in an asserted identity.

UK Level	Kantara Initiative Level	Description
0	1	Little or no confidence required
1	2	Some confidence required
2	3	High confidence required
3	4	Very high confidence required

While the numeric identifier for each level is different – the UK's system is one lower than Kantara Initiative's system – the meaning of each level is essentially the same.

Also for both the UK and Kantara Initiative, the level of assurance specifies the strength and rigour of the identity proofing process, the credential's strength, and the management processes required of the electronic trust service provider that is to provide the authentication service. Both the UK and Kantara Initiative have established service assessment criteria at each assurance level for electronic trust services providing credential management services. These service assessment criteria will be compared in later sections.

Conversely, in both the UK and Kantara Initiative, IDAs can determine the assurance level at which their services might qualify by evaluating their overall business processes and technical mechanisms against the published criteria.

OBSERVATION: Kantara Initiative's approach, while seeming to examine different aspects of the situation, covers essentially the same overall aspects as the UK's analysis with the exception of explicitly examining privacy. The aspects examined by Kantara Initiative implicitly include privacy (i.e., unauthorized release of sensitive information and Inconvenience, distress, or damage to standing or reputation) but a risk analysis process or a risk analyst could, if not privacy aware, could overlook this aspect.

The result of both risk analyses is that Service Providers identify the level of assurance they require for the electronic transaction system.

OBSERVATION: Kantara Initiative does not explicitly include privacy as one of the aspects to be examined when determining the impact of Identity Authentication Errors.

RECOMMENDATION: If the difference in numeric tags is a perceived issue the UK could change its numbering scheme. This recommendation is made (rather than Kantara Initiative changing its numbering scheme) as many other jurisdictions have already adopted the 1 to 4 designation scheme.

GPG 44

AC Element A: Credential Type

It is considered that the following Credential types, and combination of Credential types, are appropriate to support each of the authentication levels. The following table demonstrates the type of Credential required in order to meet the defined authentication levels.

Score	GPG 44 Requirement	Observations about Kantara Initiative
1	A Credential type that demonstrates the user is in possession of a Secret (e.g. a password, PIN, etc.)	LOA Level 1 and 2 check for proof of possession

	belonging to the legitimate account holder (see Annex A for further guidance on Secrets).	
2	Requirements for Score 1, plus one of the following: • A Credential type that demonstrates the user is in possession of a Secret (e.g. a password, PIN, OTP, LTS, etc.) belonging to the legitimate account holder that is exchanged over a channel that is separate to the authentication channel (see Annex A for further guidance on Secrets). • A Credential type that demonstrates the user is in possession of a biometric belonging to the legitimate account holder (see Annex D of GPG 44 for further guidance on the use of biometrics).	LOA Level 3 can include out-of-band or biometric
3	Requirements for Score 1, plus the following: • A Credential type that demonstrates the user is in possession of a hardware or software token belonging to the legitimate account holder.	LOA level 4 can utilize hardware or software tokens

OBSERVATION: Kantara Initiative has similar Service Assessment Criteria.

AC Element B: Quality of the Credential

The effectiveness of measures that the Credential employs to protect it from being predicted, duplicated or otherwise compromised are important factors in assessing its suitability for use. The following Table demonstrates the properties for the quality of the Credential and the corresponding score for this element. The Credential must, as a minimum, meet all the properties defined for the quality to achieve that score.

A Comparison of Kantara Initiative Requirements

Score	GPG 44 Requirement	Observations about Kantara Initiative
1	The Credential contains no protective measures to prevent prediction or duplication (e.g. it is a Secret that is memorised by the user). Users shall be encouraged through process, or guidance, to use Credentials with good security properties.	While LOA level 2 contains measures for resistance to online guessing attacks, there are no specific measures to prevent prediction or duplication.
2	The Credential uses measures that make it unlikely to be predicted. The Credential has measures that prevent duplication without direct access to the Credential. The Credential has measures that resist tampering. Hardware and software tokens are implemented in accordance with current Good Industry Practice (e.g. NIST SP 800-63-2) including protection against offline attack. Cryptographic modules used have been assessed as using algorithms and security measures in accordance with Good Industry Practice (e.g. FIPS 140-2 Level 2).	While LOA level 3 contains measures for resistance to online guessing attacks, there are no specific measures to prevent prediction or duplication. Hardware tokens are required to be in accordance with FIPS 140-2 Level 1 or higher. Software cryptographic tokens are required to be in accordance with FIPS 140-2 Level 1.
3	Requirements for Score 2, plus the following: • The Credential has measures that prevent duplication. • The Credential has measures that detect and prevent compromise from tampering. • Cryptographic modules used have been assessed as using algorithms and security measures in accordance with Good Industry Practice (e.g. FIPS 140-2 Level).	While LOA level 4 contains measures for resistance to online guessing attacks, there are no specific measures to prevent duplication or to detect and prevent compromise from tampering. LOA level 4 requires a cryptographic module that is validated against FIPS 140-2 3683 Level 2 or higher.

OBSERVATION: Kantara Initiative does not have service assessment criteria at any of the LOA levels to assess for specific measures to prevent prediction or duplication.

OBSERVATION: Kantara Initiative criterion in LOA level 2 does not require software cryptographic tokens to be in accordance with FIPS 140-2 Level 1 to be Level 1 or higher.

AC Element C: Management of the Credential

The confidence in the Credential is not only dependent on its properties, as the Authentication Provider must carefully manage the Credentials over their lifetime. The following Table demonstrates the required Credential management processes and the corresponding score for this element. The Authentication Provider must, as a minimum, meet all the properties defined for Credential management to achieve that score.

Score	GPG 44 Requirement	Observations about Kantara Initiative
1	The Authentication Provider stores Credentials so that they are protected from unauthorised physical and electronic access to prevent theft or damage. Further information on the storage of Credentials can be seen at Annex C. The Authentication Provider shall be able to suspend a Credential immediately from the primary system that stores the records of the currently authorised Credentials. The Authentication Provider shall be able to permanently revoke a Credential with immediate effect. The Authentication Provider shall enable the user to recover/request a replacement Credential. The Authentication Provider shall ensure that changes to the state of the Credential requested by the user can only be made by the person to whom the Credential belongs.	While LOA Level 2 does not specifically verify that Credentials are stored so that they are protected from unauthorised physical and electronic access it does require that technical controls are employed that will provide the level of security protection required by the risk assessment and the ISMS, or other IT security management methods recognized by a government or professional body. LOA Level 2 requires that changes to the state of the Credential (revocation, recovery, replacement) can only be made by the person to whom the Credential belongs. LOA Level 2 requires processes that attempt to deliver the credential into the possession of the person that requested it. While LOA level 2 does not explicitly require a credential manufacturer to have a quality management process

	The Authentication Provider shall ensure the Credential is bound to a single account. The issuing process for the Credential shall take measures that attempt to deliver it into the possession of the user that requested it. The Authentication Provider shall ensure that the Credential is under the control of the person/user to whom it belongs before, or on, first use. Where the Credential has been manufactured, the manufacturer shall have a quality management process to ensure consistency. Where the Credential uses information embedded by the manufacturer (e.g. secret number), the manufacturer shall have an information security management system which protects that information from compromise (e.g. ISO27001). Where a Credential manufacturer supplies information to the Authentication Provider, which is required as part of the Authentication, then the process for exchanging that information shall protect its integrity and confidentiality.	to ensure consistency, or an information security management system which protects information from compromise, or a process for exchanging information that protects its integrity and confidentiality, it does require that appropriate contractual arrangements are established that stipulate which critical policies, procedures, and practices a manufacturer is required to fulfill. There are no service assessment criteria that specify that: • the Authentication Provider is able to suspend a Credential immediately from the primary system that manages credentials • that the Authentication Provider be able to permanently revoke a Credential with immediate effect • the Authentication Provider ensures that the Credential is under the control of the person/user to whom it belongs before, or on, first use
2	Requirements for Score 1, plus the following: • The issuing process for the Credential shall take sufficient measures so that it can reasonably be assumed to have been delivered into the possession of the person to whom it belongs. • Where the Credential has been manufactured, the manufacturer shall have an independently	While LOA level 3 does not explicitly require a credential manufacturer to have an independently audited quality management process to ensure consistency, or an independently audited information security management system which protects that information from compromise, it does require that appropriate contractual arrangements are established that stipulate which critical policies, procedures, and

	audited quality management process to ensure consistency (e.g. ISO 9000 series). • Where the Credential uses information embedded by the manufacturer (e.g. secret number), the manufacturer shall have an independently audited information security management system which protects that information from compromise (e.g. ISO 27001).	practices a manufacturer is required to fulfill. There are no service assessment criteria that specify that the Authentication Provider has taken sufficient measures to ensure that the Credential can reasonably be assumed to have been delivered into the possession of the person to whom it belongs.
3	Requirements for Scores 1 and 2, plus the following: • The issuing process for the Credential shall take all reasonable measures to ensure it has been delivered into the possession of the person to whom it belongs. • Where the Credential has been manufactured, the manufacturer shall have an independently certified quality management process to ensure consistency under a Good Industry Practice certification scheme (e.g. ISO 9000 series). • Where the Credential uses information embedded by the manufacturer (e.g. secret number), the manufacturer shall have an independently certified information security management system which protects that information from compromise (e.g. ISO 27001).	While LOA level 4 does not explicitly require a credential manufacturer to have an independently audited quality management process to ensure consistency, or an independently audited information security management system which protects that information from compromise, it does require that appropriate contractual arrangements are established that stipulate which critical policies, procedures, and practices a manufacturer is required to fulfill. There are no service assessment criteria that specify that the Authentication Provider has taken sufficient measures to ensure that the Credential can reasonably be assumed to have been delivered into the possession of the person to whom it belongs.

OBSERVATION: Kantara Initiative service assessment criteria in LOA level 2 do not request that the Authentication Provider:

- Be able to suspend a Credential immediately from the primary system that manages credentials.
- Be able to permanently revoke a Credential with immediate effect.

- Ensures that the Credential is under the control of the person/user to whom it belongs before, or on, first use.

OBSERVATION: Kantara Initiative does not have service assessment criteria in LOA level 3 and 4 that request that the Authentication Provider has taken sufficient measures to ensure that the Credential can reasonably be assumed to have been delivered into the possession of the person to whom it belongs.

AC Element D: Monitoring

The qualities and management of the Credential contribute to its security, but it is also necessary to monitor its use. Therefore, the Authentication Provider shall monitor the use of a Credential, its services and sources to detect and react (e.g. incident management) to the misuse of a Credential. The following table demonstrates the monitoring requirements and the corresponding scores for this element. The Authentication Provider must, as a minimum, meet all the properties defined for monitoring to achieve that score.

Score	GPG 44 Requirement	Observations about Kantara Initiative
1	The Authentication Provider shall check for indications that the Credential maybe being used by someone other than its owner. Where the Authentication Provider has reasonable suspicion that the Credential is being used by someone other than its owner, the Authentication Provider shall take sufficient measures in order to determine the user is the owner of the Credential, which may include revoking and replacing the Credential.	LOA Level 2 requires the use of an authentication protocol that requires the claimant to prove possession and control of the authentication token.
2	Requirements for Score 1, plus the following: • The Authentication Provider shall take measurements to establish what normal and legitimate authentication behaviour looks like (see GPG 53), Transaction	LOA Level 3 does not require transaction monitoring and analysis to detect or report abnormal authentication behaviour.

	Monitoring for HMG Online Service Providers. • The Authentication Provider shall detect, and where applicable report, abnormal authentication behaviour (see GPG 53).	
3	Requirements for Scores 1 and 2, plus the following: • The Authentication Provider shall check HMG provided services for indications that the Credential maybe being used by someone other than its owner.	LOA Level 4 requires the use of an authentication protocol that requires the claimant to prove possession and control of the authentication token. In addition, mechanisms must be used to ensure that tokens are either still valid or have been issued within the last 24 hours.

OBSERVATION: Kantara Initiative does not have service assessment criteria in LOA level 3 and level 4 that ensure transaction monitoring and analysis take place to detect and report abnormal authentication behaviour.

AC Element E: Authentication Service Characteristics

Confidence in the use of a Credential, during the Authentication, is built upon the characteristics of the authentication service. The Authentication Provider shall ensure its authentication service protects the user, and itself, from compromise. The following Table demonstrates the required characteristics of the authentication service and the corresponding score for this element. The Authentication Provider must, as a minimum, meet all the properties defined for the authentication service characteristics to achieve that score.

Score	GPG 44 Requirement	Observations about Kantara Initiative
1	• The Authentication Provider shall design, develop, implement and maintain the technology systems that deliver its authentication services to protect the confidentiality, integrity and availability of the information processed. • The Authentication service shall	LOA Level 2 requires systems that undertake Credential Verification / Authentication. LOA Level 2 requires the service to limit the number of failed authentication attempts to no more than 100 in any 30-day period. LOA Level 2 requires the service to

	only return a success where the user has successfully authenticated using their Credential. • The Authentication service shall reject an Authentication when a suspended or revoked Credential is presented. • The Authentication service shall suspend or revoke a Credential after a number of failed Authentication attempts. • The Authentication service shall protect authentication sessions using Good Industry Practice security measures to ensure its confidentiality, integrity and authenticity and provide non-repudiation (e.g. using TLS v1.2), digital signatures FIPS 186-4. • The Authentication service shall ensure that the user can determine that they are using a secure channel to the Authentication Provider (e.g. where certificates are being used, then these are not self-signed but are signed by an industry recognised authority). • Where the Authentication service uses cryptography, then the cryptographic algorithms and keys shall be used in accordance with current Good Industry Practice. For further information, see GPG 44 Annex B.	send assertions either via a channel mutually-authenticated with the Relying Party, or signed and encrypted for the Relying Party. LOA Level 2 requires the service to apply assertion protocols which use cryptographic techniques approved by a national authority or other generally-recognized authoritative body.
2	Requirements for Score 1, plus the following: • The Authentication Provider shall use measures that are effective at preventing use by non-human operators (see Good Practice Guide 53). • The Authentication service shall use measures that prevent the	LOA level 3 ensures measures that prevent the observation and replay of Credentials that were used in a previous Authentication are used. LOA level 3 ensures measures that ensure the integrity of the information exchanged with a user are used. LOA level 3 does not have measures

	observation and replay of Credentials that were used in a previous Authentication. • The Authentication service shall use methods that ensure the integrity of the information exchanged with a user. • The Authentication service shall use measures that protect the Credential from compromise, even if the communication channel is compromised.	that are effective at preventing use by non-human operators. LOA level 3 does not have measures that protect the Credential from compromise, even if the communication channel is compromised.
3	Requirements for Scores 1 and 2, plus the following: • The Authentication service shall use measures that detect and prevent the illegitimate use of a user's Credential.	LOA level 4 requires the use of an authentication protocol that requires the claimant to prove possession and control of the authentication token thus preventing the illegitimate use of a user's Credential.

OBSERVATION: Kantara Initiative does not have service assessment criteria in LOA level 3 and 4 that check for measures that are effective at preventing use by non-human operators.

OBSERVATION: Kantara Initiative does not have service assessment criteria in LOA level 3 and 4 that check for measures that protect the Credential from compromise, even if the communication channel is compromised.

AC Element F: Information Assurance Maturity of the Authentication Provider

The information assurance maturity of the Authentication Provider is an important element in providing confidence in the delivery of the authentication service. The following Table demonstrates the information assurance maturity requirements for the Authentication Provider and the corresponding score for this element. The Authentication Provider must, as a minimum, meet all the properties defined for the information assurance maturity to achieve that score.

Score	GPG 44 Requirement	Observations about Kantara Initiative

1	• The Authentication Provider shall have an effective information security management system which protects the integrity, confidentiality and availability of its service including a forensic readiness plan. • The Authentication Provider shall have an audit regime that covers all systems supporting the use of the Credential. • The Authentication Provider shall ensure that all systems supporting the use of the Credential have a consistent time. • The Authentication Provider shall have a records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential. • The Authentication Provider shall conduct regular risk assessments and have defined processes for exception handling. • The Authentication Provider shall have a monitoring regime that detects unexpected and undesirable activity within the service. • The Authentication Provider shall have an internal monitoring regime that detects unusual, or malicious, activity of the Authentication Provider's staff and others that have physical and logical access to the systems that support the authentication service.	LOA level 2 requires the Authentication Provider to have a well-established and effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body. LOA level 2 requires the Authentication Provider to be subjected to a first-party audit at least once every 12 months for the effective provision of the specified service by internal audit functions of the enterprise responsible for the specified service. LOA level 2 does not have a specific requirement to ensure that all systems supporting the use of the Credential have a consistent time other than a requirement to ensure audit records are time stamped using a time source that is based upon an internal computer / system clock that is synchronized to an internet time source. LOA level 2 requires the Authentication Provider to demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention and destruction of private and identifiable information. This requirement does not apply to records in general. While LOA level 2 does not have a specific requirement to ensure that the Authentication Provider shall have a monitoring regime that detects unexpected and undesirable activity within the service it does require that it apply controls during system development, procurement, installation, and operation that protect

		the security and integrity of the system environment, hardware, software, and communications. While LOA level 2 does not have a specific requirement to ensure the Authentication Provider shall conduct regular risk assessments and have defined processes for exception handling it does require the Authentication Provider to demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community. LOA level 2 requires the Authentication Provider to apply controls during system development, procurement installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications. In addition, LOA level 2 requires it to apply physical access control mechanisms to ensure that: a) access to sensitive areas is restricted to authorized personnel; b) all removable media and paper documents containing sensitive information as plain-text are stored in secure containers; and c) a minimum of two persons is required to enable access to any cryptographic modules. It is also required to employ logical access control mechanisms that ensure access to sensitive system functions and controls is restricted to authorized personnel.
2	Requirements for Score 1, plus the following: • The Authentication Provider shall have an independently audited information security management	LOA level 3 requires that the Authentication Provider shall be subjected to a first-party audit at least once every 12 months for the effective provision of the specified service by internal audit functions of

	system which protects the integrity and confidentiality of its service (e.g. ISO27001), including a forensic readiness plan. • The Authentication Provider shall have an independently audited audit regime that covers all systems supporting the use of its service, including a forensic readiness plan. • The Authentication Provider shall ensure that all systems supporting the use of the Credential have a consistent accurate time using a Good Industry Practice time source. • The Authentication Provider shall have an independently audited records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential. • The Authentication Provider shall conduct regular risk assessments, and have defined processes for exception handling, using Good Industry Practice guidance (e.g. ISO 27005). • The Authentication Provider shall have an independently audited monitoring regime that detects unexpected activity within the service. • The Authentication Provider shall test its monitoring regime through a schedule of independent vulnerability and penetration tests, adjusting it to address any issues discovered. • The Authentication Provider shall have an independently audited	the enterprise responsible for the specified service. 'First-party' audits are those undertaken by an independent part of the same organization which offers the service. The auditors cannot be involved in the specification, development or operation of the service. LOA level 3 does not require that the Authentication Provider have an independently audited audit regime other than the Annual Conformance Review (ACR) that each IDA must undergo. LOA level 3 does not have a specific requirement to ensure that all systems supporting the use of the Credential have a consistent time other than a requirement to ensure audit records are time stamped using a time source that is based upon an internal computer / system clock that is synchronized to an internet time source. LOA level 3 requires the Authentication Provider to demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention and destruction of private and identifiable information. This requirement does not apply to records in general. Nor, other than under the general terms of the audit regime, that it is independently audited. LOA level 3 requires that a risk assessment review is performed at least once every six months, such as adherence to CobIT or IS27001 practices. While LOA level 3 does not have a specific requirement to ensure that

	internal monitoring regime that detects unusual, or malicious, activity of the Authentication Provider's staff and others that have physical and logical access to the systems that support the authentication service. • The Authentication Provider shall test its internal monitoring regime through a schedule of independent vulnerability and penetration tests, adjusting it to address any issues discovered.	the Authentication Provider shall have a monitoring regime that detects unexpected activity within the service it does require that it apply controls (such as a monitoring regime that detects unexpected and undesirable activity within the service) during system development, procurement, installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications. While LOA level 3 does not have a specific requirement to ensure that the Authentication Provider test its monitoring regime through a schedule of independent vulnerability and penetration tests it does require that it apply controls during system development, procurement, installation, and operation (such as independent vulnerability and penetration tests) that protect the security and integrity of the system environment, hardware, software, and communications. LOA level 3 requires the Authentication Provider to apply physical access control mechanisms to ensure that: a) access to sensitive areas is restricted to authorized personnel; b) all removable media and paper documents containing sensitive information as plain-text are stored in secure containers; and c) a minimum of two persons is required to enable access to any cryptographic modules. It is also required to employ logical access control mechanisms that ensure access to sensitive system functions and controls is restricted to authorized personnel. While LOA level 3 does not have a

		specific requirement to ensure that the Authentication Provider test its internal monitoring regime through a schedule of independent vulnerability and penetration tests it does require that it apply controls during system development, procurement, installation, and operation (such as independent vulnerability and penetration tests) that protect the security and integrity of the system environment, hardware, software, and communications.
.3	Requirements for Scores 1 and 2, plus the following: • The Authentication Provider shall have an independently certified information security management system which protects the integrity and confidentiality of its service (e.g. ISO 27001), including a forensic readiness plan. • The Authentication Provider shall have an independently certified audit regime that covers all systems supporting the use of the Credential (e.g. ISO 27001). • The Authentication Provider shall ensure that all systems supporting the use of the Credential have a consistent and accurate time synchronised from a Stratum 1 time source (or equivalent). • The Authentication Provider shall have an independently certified records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential (e.g. ISO 15489).	While LOA level 4 does not specifically require that the Authentication Provider have an independently certified information security management system which protects the integrity and confidentiality of its service it does require it to have in place an Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body, that follows best practices as accepted by the information security industry and that applies and is appropriate to the IDA in question. While LOA level 4 does not specifically require that the Authentication Provider have an independently certified audit regime that covers all systems supporting the use of the Credential it does require it to have in place an Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body, that follows best practices as accepted by the information security industry and that applies and is appropriate to the IDA

		in question. These practices can specify the requirement for an independently certified audit regime. LOA level 4 does requires that the Authentication Provider shall be subjected to a first-party audit at least once every 12 months for the effective provision of the specified service by internal audit functions of the enterprise responsible for the specified service. 'First-party' audits are those undertaken by an independent part of the same organization which offers the service. The auditors cannot be involved in the specification, development or operation of the service. LOA level 4 does not have a specific requirement to ensure that all systems supporting the use of the Credential have a consistent time other than a requirement to ensure audit records are time stamped using a time source that is based upon an internal computer / system clock that is synchronized to a trusted internet time source which could be a Stratum 1 (or equivalent) time source. While LOA level 4 does not specifically require that the Authentication Provider have an independently certified records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential it does require it to have in place an Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body, that follows best practices as accepted by the

		information security industry and that applies and is appropriate to the IDA in question. These practices can specify the requirement for an independently certified records management system.

OBSERVATION: Kantara Initiative does not have service assessment criteria in LOA level 2 that check that all systems supporting the use of the Credential have a consistent time.

OBSERVATION: Kantara Initiative does not have service assessment criteria in LOA level 2 that check that an Authentication Provider has a records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential.

OBSERVATION: Kantara Initiative does not have service assessment criteria in LOA level 3 that check that all systems supporting the use of the Credential have a consistent time using a Good Industry Practice time source.

OBSERVATION: Kantara Initiative service assessment criteria in LOA level 4 concerning information security management system do not specify that it should be independently certified.

OBSERVATION: Kantara Initiative service assessment criteria in LOA level 4 concerning information security management system do not explicitly identify that it should include an independently certified audit regime.

OBSERVATION: Kantara Initiative service assessment criteria in LOA level 4 concerning information security management system do not explicitly identify that it should include an independently certified records management system.

OBSERVATION: Kantara Initiative does not have service assessment criteria in LOA level 4 that check that all systems supporting the use of the Credential have a consistent time using a trusted Industry Practice time source such as Stratum 1 (or equivalent).

RECOMMENDATION: Kantara Initiative considers adding an example to the service assessment criteria in LOA level 2 that check that an Authentication Provider applies controls during system development, procurement, installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications to specifically mention a monitoring regime that detects unexpected and undesirable activity within the service.

RECOMMENDATION: Kantara Initiative considers adding an example to the service assessment criteria in LOA level 2 that check that an Authentication Provider demonstrates a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community to specifically mention the conduct of regular risk assessments and the handling of exceptions.

RECOMMENDATION: Kantara Initiative considers modifying the service assessment criteria in LOA level 3 and level 4 concerning Internal Service Audit to Service Audit. Additionally, the description should include provision of either a first-party audit or an independent audit at least once every 12 months. The description of the service assessment criteria should also make mention of a forensic readiness plan.

RECOMMENDATION: Kantara Initiative considers adding an example to the service assessment criteria in LOA level 3 that check that an Authentication Provider to demonstrate that it applies controls during system development, procurement, installation, and operation that protect the security and integrity of the system environment, hardware, software, and communications to specifically mention a monitoring regime that detects unexpected activity within the service and includes a schedule of independent vulnerability and penetration tests.

RECOMMENDATION: Kantara Initiative considers adding an example to the service assessment criteria in LOA level 3 that check that an Authentication Provider provides physical and logical access control to specifically mention an independently audited internal monitoring regime that detects unusual, or malicious, activity of the Authentication Provider's staff and others as well as the inclusion of a schedule of independent vulnerability and penetration tests.

GPG 45 Compliance

IPV Element A – Strength of Identity Evidence

The purpose of this element is to record the strength of the Identity Evidence provided by the Applicant in support of the Claimed Identity. The following Table demonstrates the properties of the Identity Evidence and the corresponding score for this element. The Identity Evidence must, as a minimum, meet all the properties defined for a particular strength to achieve that score. The IPV Operations Manual provides additional details on techniques and technical requirements for this element. These details are beyond the scope of this high level review.

Score	GPG 45 Requirements	Observations about Kantara Initiative

0	No compliant Identity Evidence provided	Not applicable
1	The issuing source of the Identity Evidence performed no identity checking The issuing process for the Identity Evidence means that it can reasonably be assumed to have been delivered into the possession of an individual The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates OR The issued Identity Evidence contains a photograph / image / Biometric of the person to whom it relates	For LOA level 1 the service must include in its Service Definition a. at least one of the following classes of identity proofing service; i. "In-Person Public Identity Proofing"; or ii. "Remote Public Identity Proofing". b. may offer any additional classes of identity proofing service it chooses, subject to the nature and the entitlement of the IDA concerned; and c. must fulfill the applicable assessment criteria according to its choice of identity proofing service. *In-Person Public Identity Verification* requires self-assertion of identity and self-attestation of evidence. *Remote Public Identity Verification* requires the applicant to provide a contact telephone number or email address which is verified by calling the number or by successfully sending a confirmatory email and receiving a positive acknowledgement. *NOTE*: Where the Applicant already possesses recognized original credentials, the IDA may choose to accept the verified identity of the Applicant as a substitute for identity proofing, subject to proving that the original credential on which the identity-proofing relies is in the possession and under the control of the Applicant. All other requirements

		of LOA level 1 identity proofing must also be observed.
2	The Issuing Source of the Identity Evidence confirmed the applicant's identity through an identity checking process The issuing process for the Identity Evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates OR The issued Identity Evidence contains a photograph / image / Biometric of the person to whom it relates Where the issued Identity Evidence is, or includes, electronic information that information is protected using cryptographic methods and those methods ensure the integrity of the information and enable the authenticity of the claimed Issuing Source to be confirmed Where the issued Identity Evidence is, or includes, a physical object it requires Proprietary Knowledge to be able to reproduce it	For LOA level 2 the enterprise or specific service: a. must include in its Service Definition at least one of the following classes of identity proofing service; i. "In-Person Public Identity Verification"; ii. "Remote Public Identity Verification"; iii. "Current Relationship Identity Verification"; iv. "Affiliation Identity Verification"; b. may offer any additional classes of identity proofing service it chooses, Subject to the nature and the entitlement of the IDA concerned; and c. must fulfill the applicable assessment criteria according to its choice of identity proofing service. *In-Person Public Identity Verification* requires that the applicant is in possession of a primary Government Picture identification document that bears a photographic image of the holder which is verified by processes that ensure that the presented document: d. appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application; e. bears a photographic image of the holder that matches that of

		the applicant; and f. provides all reasonable certainty that the identity exists and that it uniquely identifies the applicant. *Remote Public Identity Verification* requires the applicant to submit references of and attests to current possession of a primary Government identification document, and one of: g. a second Government identification; h. an employee or student identity number; i. a financial account number (e.g., checking account, savings account, loan or credit card) or; j. a utility service account number (e.g., electricity, gas, or water) for an address matching that in the primary document; k. a telephone service account. Ensure that the applicant provides additional verifiable personal information that at a minimum must include: l. a name that matches the referenced photo-identification; m. date of birth and; n. current address; o. for a telephone service account, the demonstrable ability to send or receive messages at the phone number. The information is verified by inspection and analysis of records against the provided identity references with the specified issuing authorities/institutions or through

		similar databases, according to the inspection rules set by the issuing authorities. *Current Relationship Identity Proofing* requires the IDA to have previously exchanged a shared secret (e.g., a PIN or password) with the applicant that meets LOA level 2 (or higher) entropy requirements which is verified by ensuring that it only issued the shared secret after originally establishing the applicant's identity or it has an ongoing business relationship sufficient to satisfy the enterprise of the applicant's continued personal possession of the shared secret. *Affiliation Identity Proofing* requires that the applicant possesses: a) verified identification from the organization with which it is claiming affiliation; and b) verified agreement from the organization that the applicant may be issued a credential indicating that an affiliation exists. *Identity-proofing based on Recognized Credentials* requires that, prior to issuing any derived credential, the original credential on which the identity-proofing relies must be: p. authenticated by a source trusted by the IDA as being valid and un-revoked; q. issued at LOA Level 3 or 4; r. issued in the same name as that which the Applicant is claiming; s. proven to be in the possession and under the control of the Applicant.
3	The Issuing Source of the Identity	For LOA level 3 the enterprise or

	Evidence confirmed the applicant's identity in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2007 The issuing process for the Identity Evidence ensured that it was delivered into the possession of the person to whom it relates The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates The Personal Name on the issued Identity Evidence must be the name that the identity was officially known at the time of issuance. Pseudonyms, aliases and initials for forenames and surnames are not permitted The issued Identity Evidence contains a photograph/image/Biometric of the person to whom it relates **OR** The ownership of the issued Identity Evidence can be confirmed through Knowledge Based Verification Where the issued Identity Evidence is, or includes, electronic information that information is protected using cryptographic methods and those methods ensure the integrity of the information and enable the authenticity of the claimed Issuing Source to be confirmed Where the issued Identity Evidence is, or includes, a physical object it contains developed security features that requires Proprietary Knowledge and Proprietary Apparatus to be able to reproduce it	specific service: t. must include in its Service Definition at least one of the following classes of identity proofing services, and; u. may offer any additional classes of identity proofing service it chooses, Subject to the nature and the entitlement of the IDA concerned; v. must fulfill the applicable assessment criteria according to its choice of identity proofing service, i.e. conform to at least one of the service assessment criteria sets defined in: i. "In-Person Public Identity Verification"; ii. "Remote Public Identity Verification"; iii. "Current Relationship Identity Verification"; iv. "Affiliation Identity Verification". *In-Person Public Identity Verification* requires that the applicant is in possession of a primary Government Picture identification document that bears a photographic image of the holder which is verified by processes that ensure that the presented document: w. appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application; x. bears a photographic image of the holder that matches that of the applicant; y. is electronically verified by a

		record check with the specified issuing authority or through similar databases that: i. establishes the existence of such records with matching name and reference numbers; ii. corroborates date of birth, current address of record, and other personal information sufficient to ensure a unique identity; z. provides all reasonable certainty that the identity exists and that it uniquely identifies the applicant. *Remote Public Identity Verification* requires the applicant to submit references of and attests to current possession of a primary Government identification document, and one of: aa. a second Government identification; bb. an employee or student identification number; cc. a financial account number (e.g., checking account, savings account, loan, or credit card), or; dd. a utility service account number (e.g., electricity, gas, or water) for an address matching that in the primary document. ee. Ensure that the applicant provides additional verifiable personal information that at a minimum must include: ff. a name that matches the referenced photo-identification; gg. date of birth; hh. current address.

		The provided information is electronically verified by a record check against the provided identity references with the specified issuing authorities / institutions or through similar databases, according to the inspection rules set by the issuing authorities. *Current Relationship Identity Proofing* requires the IDA to have previously exchanged a shared secret (e.g., a PIN or password) with the applicant that meets LOA level 3 (or higher) entropy requirements which is verified by ensuring that it only issued the shared secret after originally establishing the applicant's identity or it has an ongoing business relationship sufficient to satisfy the enterprise of the applicant's continued personal possession of the shared secret. *Affiliation Identity Proofing* requires that the applicant possesses: a) verified identification from the organization with which it is claiming affiliation; and b) verified agreement from the organization that the applicant may be issued a credential indicating that an affiliation exists. *Identity-proofing based on Recognized Credentials* requires that, prior to issuing any derived credential, the original credential on which the identity-proofing relies must be: ii. authenticated by a source trusted by the IDA as being valid and un-revoked; jj. issued at LOA level 4; kk. issued in the same name as that which the Applicant is claiming;

		ll. proven to be in the possession and under the control of the Applicant.
4	The Issuing Source of the Identity Evidence confirmed the applicant's identity in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2007 The Issuing Source visually identified the applicant and performed further checks to confirm the existence of that identity The issuing process for the Identity Evidence ensured that it was delivered into the possession of the person to whom it relates The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates The Personal Name on the issued Identity Evidence must be the name that the identity was officially known at the time of issuance. Pseudonyms, aliases and initials for forenames and surnames are not permitted The issued Identity Evidence contains a photograph / image of the person to whom it relates The issued Identity Evidence contains a Biometric of the person to whom it relates Where the issued Identity Evidence is, or includes, electronic information that information is protected using cryptographic methods and those methods ensure the integrity of the information and enable the authenticity of the claimed Issuing Source to be confirmed	For LOA level 4 the enterprise or specific service may only offer face-to-face identity proofing service. *In-Person Public Identity Verification* requires that the applicant is in possession of: mm. a primary Government Picture identification document that bears a photographic image of the holder and either: i. secondary Government Picture identification or an account number issued by a regulated financial institution or; ii. two items confirming name, and address or telephone number, such as: utility bill, professional license or membership, or other evidence of equivalent standing. iii. The primary identification is verified by ensuring that the presented document: nn. appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application; oo. bears a photographic image of the holder which matches that of the applicant; pp. is electronically verified by a record check with the specified issuing authority or through similar databases that: i. establishes the existence of

	Where the issued Identity Evidence is, or includes, a physical object it contains developed security features that requires Proprietary Knowledge and Proprietary Apparatus to be able to reproduce it.	such records with matching name and reference numbers; ii. corroborates date of birth, current address of record, and other personal information sufficient to ensure a unique identity; qq. provides all reasonable certainty, at LOA level 4, that the identity exists and that it uniquely identifies the applicant. The secondary identification is verified by ensuring that the presented document meets the following conditions: rr. If it is secondary Government Picture identification: i. appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application; ii. bears a photographic image of the holder which matches that of the applicant; iii. states an address at which the applicant can be contacted. ss. If it is a financial institution account number, is verified by a record check with the specified issuing authority or through similar databases that: i. establishes the existence of such records with matching name and reference numbers; ii. corroborates date of birth, current address of record, and other personal information sufficient to ensure a unique

		identity. tt. If it is two utility bills or equivalent documents: i. each appears to be a genuine document properly issued by the claimed issuing authority; ii. corroborates current address of record or telephone number sufficient to ensure a unique identity.

OBSERVATION: Kantara Initiative service assessment criteria at LOA level 1 In-Person Public Identity Proofing specify self-assertion of identity and self-attestation of evidence instead of the examination, but not validation or verification, of identity evidence and that the Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates or a photograph / image / Biometric of the person to whom it relates.

OBSERVATION: UK requirements do not separate “In-Person Public Identity Verification”; “Remote Public Identity Verification”; “Current Relationship Identity Verification”; and “Affiliation Identity Verification”.

OBSERVATION: Kantara Initiative service assessment criteria at LOA level 4 In-Person Public Identity Proofing do not include a requirement that issued Identity Evidence contains a Biometric of the person to whom it relates.

RECOMMENDATION: Additional analysis is required to determine if the identity proofing activities required by Kantara Initiative to meet LOA level 3 and 4 requirements satisfy UK Money Laundering Regulations 2007.

IPV Element B – Outcome of the Validation of Identity Evidence

The purpose of this element is to record the score obtained from the Identity Evidence Validation process. The following table demonstrates the characteristics of the Validation processes and the corresponding score for this element. The IPV Operations Manual provides additional details on techniques and technical requirements for this element. These details are beyond the scope of this high level review.

Score	GPG 45 Requirement	Observations about Kantara Initiative
0	Validation of the Identity Evidence was unsuccessful	Not Applicable
1	All Personal Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source	Kantara Initiative provides mechanisms to validate information provided by the applicant depending on the information that has been provided for a specific LOA level.
2	All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held / published by the Issuing / Authoritative Source **OR** The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skill and appropriate equipment and confirmed the integrity of the physical security features **OR** The issued Identity Evidence has been confirmed as Genuine by confirmation of the integrity of the cryptographic security features	Kantara Initiative provides mechanisms to validate information provided by the applicant depending on the information that has been provided for a specific LOA level.
3	The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skill and appropriate equipment and confirmed the integrity of the physical security features **OR** The issued Identity Evidence has been confirmed as Genuine by confirmation of the integrity of the cryptographic security features **AND** All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by	Kantara Initiative provides mechanisms to validate information provided by the applicant depending on the information that has been provided for a specific LOA level.

	comparison with information held/published by the Issuing/Authoritative Source **OR** Evidence Details from the Identity Evidence have been confirmed as not known to be invalid by comparison with information held/published by the Issuing Source/Authoritative Source	
4	The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skill and appropriate equipment including the integrity of any cryptographic security features **AND** All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing Source/Authoritative Source	Kantara Initiative provides mechanisms to validate information provided by the applicant depending on the information that has been provided for a specific LOA level.

RECOMMENDATION: Additional analysis, beyond the scope of this study, is required to determine if the mechanisms specified by Kantara Initiative to validate information provided by the applicant at each LOA level meet the requirements identified in GPG 45.

IPV Element C – Outcome of Identity Verification

The purpose of this element is to record the score obtained from the Identity Verification process. The following table demonstrates the outcomes of the Verification processes and the corresponding score for this element. The IPV Operations Manual provides additional details on techniques and technical requirements for this element. These details are beyond the scope of this high level review.

Score	Identity Verification Outcome	Observations about Kantara Initiative
0	Unable to confirm that the Applicant is the owner of the Claimed Identity	Not Applicable

1	The Applicant has been confirmed as having access to the Identity Evidence provided to support the Claimed Identity	Kantara Initiative provides mechanisms to verify information provided by the applicant depending on the information that has been provided for a specific LOA level.
2	The Applicant's ownership of the Claimed Identity has been confirmed by a Static Knowledge Based Verification **OR** The Applicant's ownership of the Claimed Identity has been confirmed by a Dynamic Knowledge Based Verification **OR** The Applicant's ownership of the Claimed Identity has been confirmed by a physical comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity **OR** The Applicant's ownership of the Claimed Identity has been confirmed by a Biometric comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity	Kantara Initiative provides mechanisms to verify information provided by the applicant depending on the information that has been provided for a specific LOA level.
3	The Applicant's ownership of the Claimed Identity has been confirmed by physical comparison using a photograph/image **OR** Biometric comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity **AND** The Applicant's ownership of the Claimed Identity has been confirmed by a Static **OR** Dynamic Knowledge	Kantara Initiative provides mechanisms to verify information provided by the applicant depending on the information that has been provided for a specific LOA level.

	Based Verification	
4	The Applicant's ownership of the Claimed Identity has been confirmed by a physical comparison of the Applicant using a photograph/image to the strongest pieces of Identity Evidence **OR** By a Biometric comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity **AND** The Applicant's ownership of the Claimed Identity has been confirmed by both a Static **AND** Dynamic Knowledge Based Verification **AND** The Applicant's ownership of the Claimed Identity has been confirmed by an interaction with the Applicant via the declared address	Kantara Initiative provides mechanisms to verify information provided by the applicant depending on the information that has been provided for a specific LOA level.

RECOMMENDATION: Additional analysis, beyond the scope of this study, is required to determine if the mechanisms specified by Kantara Initiative to verify information provided by the applicant at each LOA level meet the requirements identified in GPG 45

IPV Element D – Outcome of Counter-Fraud Checks

The purpose of this element is to record the score obtained from the Counter-Fraud Check process. The following Table demonstrates the outcomes and the corresponding score once any investigation activity has been carried out for this element. The IPV Operations Manual provides additional details on techniques and technical requirements for this element. These details are beyond the scope of this high level review.

Score	Counter-Fraud Checks	Observations about Kantara Initiative
0	Applicant is suspected of being, or	Kantara Initiative does not explicitly

	known to be, fraudulent	undertake Counter-Fraud Checks for any LOA level.
1	No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity	Kantara Initiative does not explicitly undertake Counter-Fraud Checks for any LOA level.
2	No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity **AND** No confirmed evidence, using a reliable and independent source, that the Applicant is fraudulent	Kantara Initiative does not explicitly undertake Counter-Fraud Checks for any LOA level.
3	No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity **AND** No confirmed evidence, using a reliable and independent source, that the Applicant is fraudulent **AND** No confirmed evidence, using HMG specified source(s), that the Applicant is fraudulent	Kantara Initiative does not explicitly undertake Counter-Fraud Checks for any LOA level.
4	No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity **AND** No confirmed evidence, using a reliable and independent source, that the Applicant is fraudulent **AND** No confirmed evidence, using HMG specified source(s), that the Applicant	Kantara Initiative does not explicitly undertake Counter-Fraud Checks for any LOA level.

	is fraudulent **AND** No confirmed evidence, using source(s) private to HMG, that the Applicant is fraudulent	

RECOMMENDATION: Additional analysis, beyond the scope of this study, is required to determine how Counter-Fraud Checks can be added to the Kantara Initiative service assessment criteria at each LOA level in order to satisfy the requirements identified in GPG 45.

IPV Element E – Activity History of the Claimed Identity

The purpose of Activity History is to prove a continuous existence of the Claimed Identity over a period of time backwards from the point of Assessment. Activity History is determined by collating Activity Events across multiple Evidence Categories into a single Activity Event Package.

To qualify, the Activity Event shall relate to an interaction between the Claimed Identity and a source of Activity Events. This can be in either direction, e.g. the Claimed Identity using the services of the source or the source initiating an interaction with the Claimed Identity including issuing something to the Claimed Identity. Activity Event data must refer to an individual whose Personal Details match those of the Claimed Identity, allowing for any changes in Claimed Identity that have occurred over the time period being assessed for the Activity History.

The degree of assurance that can be taken from the Activity History process is linked to the quality of the data used, how easily it can be fabricated and how well its integrity is protected. The proofing organisation shall take this in to account when assessing the Activity History, expanding the data sources and extending the history period where there is insufficient confidence in the Activity Events.

The proofing organisation shall be able to demonstrate with the Activity Events a continuous existence of the Claimed Identity over the period required by the Identity Level.

The following table describes the scoring profile for this element.

Score	Properties of Activity History	Observations about Kantara Initiative

0	Unable to demonstrate the required Activity History	Kantara Initiative does not explicitly undertake checks of activity history for any LOA level.
1	No demonstration of an Identity's Activity History was required	Kantara Initiative does not explicitly undertake checks of activity history for any LOA level.
2	Claimed Identity demonstrates an Activity History of at least 180 calendar days	Kantara Initiative does not explicitly undertake checks of activity history for any LOA level.
3	Claimed Identity demonstrates an Activity History of at least 405 calendar days	Kantara Initiative does not explicitly undertake checks of activity history for any LOA level.
4	Claimed Identity demonstrates an Activity History of at least 1080 calendar days	Kantara Initiative does not explicitly undertake checks of activity history for any LOA level.

RECOMMENDATION: Additional analysis, beyond the scope of this study, is required to determine how Activity History of the Claimed Identity can be added to the service assessment criteria at each LOA level in order to satisfy the requirements identified in GPG 45.

Specification for Organisations Providing Proofing and Authentication of Digital Identities

Eligibility Requirement	Observations about Kantara Initiative
Organisations shall demonstrate that they are able to meet the requirements of this Specification through the achievement of certification by a Certification Body in accordance with the certification specification.	Kantara Initiative has a similar requirements
Organisations shall provide all information required by the Certification Body to meet their obligations in respect of identity proofing and authentication of individuals.	Kantara Initiative has a similar requirements
Organisations shall provide the Certification Body with a detailed	An organizations is required, at all LOA levels, to make available a Service

description of their Identity Assurance Service.	Definition for the specified service.

Changes to Eligibility Status Requirements	Observations about Kantara Initiative
Organisations that have been suspended by one Certification Body, due to a failure to implement the requirement in this specification, shall not be allowed to practice for any other Certification Body until that suspension is revoked and the requirements are met.	Kantara Initiative does not have this requirement
Should Identity Providers wish to transfer between certification bodies, they shall be allowed to do so subject to conditions laid down in the certification specification.	An organization, at all LOA levels, must be assessed by Kantara Assessors.
Organisations shall inform their Certification Body of any significant changes on their service post certification. In such cases the Certification Body shall decide whether full recertification is required or any additional checks need to be completed. When an Organisation requests to extend their certification scope, for example Organisations that are certified to deliver services at LOA level 2 wishing to deliver services at LOA level 3, a full recertification audit shall be required.	An organization is required, at all LOA levels, to inform Kantara Initiative of any significant changes on their service post certification. In addition, an organization must have an Annual Conformance Review performed.
Organisations shall ensure that they have arrangements to cover liability for the entirety of the Service undertaken under the scope of this Specification. Organisations shall ensure any policy is issued by an insurer included on the Financial Services Authority (FSA) register as 'Authorised', 'EEA 12 Authorised' or 'Appointed Representative' and provide the Certification Body with certificates of insurance at the initial certification, surveillance audit and on renewal of any insurance policy.	An organization is required, at all LOA levels, to provide documentation of financial resources that allow for the continued operation of the service and demonstrate appropriate liability processes and procedures that satisfy the degree of liability exposure being carried.

Organisations surrendering their certification under this Specification shall ensure indemnity cover of at least six years is provided for any identities proofed or authenticated. This may be in the form of an on-going indemnity policy or run off cover. Failure to comply with this requirement may result in civil action being taken against the Organisation.	However, an organization must define, at all LOA levels, the practices in place for the protection of Subjects' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally required records and for the secure destruction and disposal of any such information whose retention is no longer legally required. Specific details of these practices must be made available.

Robust and Credible Management Systems Requirements	Observations about Kantara Initiative
Organisations shall have documented procedures in place that can implement the requirements of this Specification and shall review their procedures in response to any change to the Identity Assurance Assessment process or this Specification.	An organization must meet this requirement in order to be approved**.**
Organisations shall have an Information Security Management System (ISMS) and demonstrate to the CB that they meet a recognised standard for ISMS e.g. ISO27001.	An organization is required, at LOA levels 2, 3 and 4, to have a well-established and effective Information Security Management System (ISMS), or other IT security management methodology recognized by a government or professional body.
Organisations shall have a quality management system and demonstrate to the CB that they meet a recognised standard for Quality Management e.g. ISO9001.	An organization is required, at LOA levels 2, 3 and 4, to demonstrate that there is in place a quality management system that is appropriate for the specified service.
All Organisations shall have written procedures for dealing with the following activities: uu. Control of documents; vv. Control of records; ww. Control of non-conforming	Kantara Initiative has a similar requirements

services; xx. Corrective action; yy. Preventative action; zz. Internal audit; aaa. Management review.	
Organisations shall establish and maintain records in relation to each Identity Assurance Assessment undertaken containing at least the following information: bbb. Name ccc. Address ddd. Date of Birth eee. Gender fff. Evidence details ggg. The explicit consent to gather and use customer data for the service	An organization must show, at all LOA levels, that it applies identity proofing policies and procedures and that it retains appropriate records of identity proofing activities and evidence. The specific content of these records is not specified.
Organisations shall ensure that all information associated with the provision of the Service is securely stored for a minimum of seven years regardless of whether user chooses to cease using the identity services of the IDA. Organisations shall also make this information available to the Identity Assurance programme when requested.	An organization must specifically set out and demonstrate, at all LOA levels, that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention and destruction of private and identifiable information (personal and business - i.e. its secure storage and protection against loss, accidental public exposure, and/or improper destruction) and the protection of Subjects' private information (against unlawful or unauthorized access, excepting that permitted by the information owner or required by due process).
Organisations shall have systems to ensure compliance with the relevant data protection legislation within the UK and register with the Public Register of Data Controllers by notifying the Information Commissioner's Office (ICO). In particular,	An organization must specifically set out and demonstrate, at all LOA levels, that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention and destruction of private and

Organisations shall ensure that information obtained through the Identity Assurance process remains confidential outside of requirements to provide that information to the following parties: hhh. The Identity Assurance Programme; iii. Where required, the Certification Body; jjj. As covered by the Data Protection Act;	identifiable information (personal and business - i.e. its secure storage and protection against loss, accidental public exposure, and/or improper destruction) and the protection of Subjects' private information (against unlawful or unauthorized access, excepting that permitted by the information owner or required by due process).
Organisations will only process personal data in accordance with the Data Protection Act 1998, or EU Member State national equivalent.	An organization must specifically set out and demonstrate, at all LOA levels, that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention and destruction of private and identifiable information (personal and business - i.e. its secure storage and protection against loss, accidental public exposure, and/or improper destruction) and the protection of Subjects' private information (against unlawful or unauthorized access, excepting that permitted by the information owner or required by due process).
Organisations shall agree to their current or past Certification Body sharing information with other Certification Bodies and other relevant third parties where appropriate, to allow for investigation of: kkk. Their compliance with the requirements of this Specification; lll. Any on-going or completed disciplinary actions; mmm. Complaints against the Organisation or their staff; nnn. The outcome of any monitoring undertaken by Certification Bodies.	Kantara does not have a similar requirement

Internal Audit and Corrective Action	Observations about Kantara Initiative
Organisations shall keep a schedule of audits to be undertaken to check compliance with this Specification and shall keep records of such audits and any resulting actions. This shall ensure that at least five per cent of Identities proofed are internally audited within a 12-month period.	An organization, at all LOA levels, must undergo an Annual Conformance Review. An organization, at all LOA levels, is not required to ensure that at least five per cent of Identities proofed are internally audited within a 12-month period.
Organisations shall identify and systematically examine the cause and consequences of any issues raised during internal audits and document the findings.	An organization, at all LOA levels, is not required to identify and systematically examine the cause and consequences of any issues raised during internal audits and document the findings.
Organisations shall carry out corrective actions including rectification of the particular occurrence(s) identified during internal audits and initiate measures to prevent recurrence.	An organization, at all LOA levels, is not required to carry out corrective actions including rectification of the particular occurrence(s) identified during internal audits and initiate measures to prevent recurrence.

Complaints Management Requirements	Observations about Kantara Initiative
Organisations shall have in place and operate a documented complaints procedure appropriate for the following activities: ooo. Receiving, recording, acknowledging and resolving all complaints from customers. The records shall include actions taken to resolve issues that have been the subject of a complaint and of the outcome including evidence that the complainant is satisfied with the outcome; ppp. Receiving, recording and addressing complaints from the IDA Service. The records shall include actions taken to resolve issues that have been the subject of a complaint and of the outcome including evidence	An organization, at all LOA levels, is not required to have in place and operate a documented complaints procedure.

that the complainant is satisfied with the outcome; qqq. Informing their customers what the procedures are and what further recourse is available, including informing their customers that accessing the complaints procedures does not affect their statutory rights; rrr. Informing their Certification Body of all complaints including details of the issue(s) resolved and disclose all material correspondence and other evidence if requested; sss. Acknowledging a complaint within seven days and escalating the complaint if it is not resolved in line with the Service Delivery Requirements, including the customer's right to take the matter the Certification Body.	

Operational Procedures	Observations about Kantara Initiative
Organisations shall demonstrate to Certification bodies how they meet the requirements of the following documents, to the version that has been stated in the service description. ttt. Good Practice Guide 44; uuu. Good Practice Guide 45; vvv. IPV Operations Manual; www. Service Delivery Requirements; xxx. Good Practice Guide 53.	An organization must meet this requirement in order to be approved**.**
Organisations shall have a documented process to register applications that meets the requirements as defined in the latest version of the IPV Operations Manual and Service Delivery Requirements.	An organization must, at all LOA levels, make available to the intended user community a Service Definition that includes all applicable Terms, Conditions, and Fees, including any limitations of its usage. The Service Definition could include the process to register

	applications.
Organisations shall have a documented process to determine that the evidence supplied by a customer, to support their claimed identity, that meets the required level for IPV Element A, as defined in the latest version of GPG 45 and the IPV Operations Manual.	See IPV Element A under GPG 45
Organisations shall have a documented process to determine that the evidence supplied by a customer, to support their claimed identity, is valid and meets the required level for IPV Element B as defined in the latest version of GPG 45 and the IPV Operations Manual.	See IPV Element B under GPG 45
Organisations shall have a documented process to determine that the evidence supplied by a customer, to support their claimed identity, has been linked to the individual, through verification. The process shall meet the required level for IPV Element C as defined in the latest version of GPG 45 and the IPV Operations Manual.	See IPV Element C under GPG 45
Organisations shall have a documented process to detect if the evidence supplied by a customer or the customer themselves, have indicators of fraud or fraudulent use against them. This process shall include the actions required to determine whether the customer is acting fraudulently or not and the reporting mechanisms both internally and externally as required. The process shall meet the required level for IP Element D as defined in the latest version of GPG 45 and IPV Operations Manual.	See IPV Element D under GPG 45
Organisations shall have a documented process to determine that the activity history of the identity has been checked to the required level for IPV Element E as defined in the latest version of GPG 45 and IPV Operations Manual.	See IPV Element E under GPG 45

Organisations shall have a documented process to determine that the authentication mechanism used to identify a returning customer meets the required level as defined in the latest version of GPG 44 and IPV Operations Manual.	See GPG 44
Organisations will have documented processes for the management of authentication including issuance, activation, misuse detection, revocation, and renewal, as defined in the latest version of GPG 44 and IPV Operations Manual.	See GPG 44
Organisations shall have a documented process for Transactional Monitoring of the use of the credential and the identity when they are interacting with a customer as defined in the latest version of GPG 44 and GPG 53.	See GPG 44
Organisations shall have a documented process to define how and what they will report to the IDA service or other Organisations, security incidents and suspect fraudulent activity that they detects in relation to the IDA Service. This will include other systems within the Organisation that interconnects or impacts on the IDA Service.	An organization, at all LOA levels, is not required to have a documented process to define how and what they will report to the IDA service or other Organisations, security incidents and suspect fraudulent activity that they detects in relation to the IDA Service.
Organisations shall have documented procedures to meet the requirements laid down within the latest version of the Operations Manual.	See GPG 45.
Organisations shall have documented procedures to meet the requirements laid down within the latest version of the Service Delivery Requirements.	See Service Delivery Requirements.
Organisations shall demonstrate to the Auditors, how these processes are implemented and demonstrate their compliance with their own processes.	An organization must meet this requirement in order to be approved**.**

OBSERVATION: Kantara Initiative does not have service assessment criteria to ensure that an organization that has been suspended by one Certification Body, due to a failure to implement the requirement in this specification, shall not be allowed to practice for any other Certification Body until that suspension is revoked and the requirements are met.

OBSERVATION: Kantara Initiative does not have service assessment criteria to ensure that an organization agrees to their current or past Certification Body sharing information with other Certification Bodies and other relevant third parties where appropriate.

OBSERVATION: Kantara Initiative does not have service assessment criteria to ensure that at least five per cent of Identities proofed are internally audited within a 12-month period.

OBSERVATION: Kantara Initiative does not have service assessment criteria to ensure that an organization is required to identify and systematically examine the cause and consequences of any issues raised during internal audits and document the findings.

OBSERVATION: Kantara Initiative does not have service assessment criteria to ensure that an organization is required to carry out corrective actions including rectification of the particular occurrence(s) identified during internal audits and initiate measures to prevent recurrence.

OBSERVATION: Kantara Initiative does not have service assessment criteria to ensure that an organization is required to have in place and operate a documented complaints procedure.

OBSERVATION: Kantara Initiative does not have service assessment criteria to ensure that an organization is required to have a documented process to define how and what they will report to the IDA service or other Organisations, security incidents and suspect fraudulent activity that they detects in relation to the IDA Service.

RECOMMENDATION: Kantara Initiative should create a profile for the UK that specifies that the indemnity should cover of at least six years is provided for any identities proofed or authenticated.

Specification for Certification Bodies Certifying Identity Assurance Providers

Requirements	Observations about Kantara Initiative
Certification Bodies must achieve United Kingdom Accreditation Service (UKAS) accreditation against BS EN ISO/IEC 17065 which consists of the following 13	Kantara Initiative's Assurance Assessment Scheme consists of the following process / requirements certifying an IDA:

steps / requirements: • General • Application • Application Review • Evaluation • Review • Certification Decision • Certification Documentation • Directory of Certified Products • Surveillance • Changes Affecting Certification • Termination, Reduction, Suspension or Withdrawal of Certification • Records • Complaints and Appeals	• Receipt of Applications • Evaluation of Applications • Grant of Rights of Use (to the Kantara Initiative Mark) • Appeal of Decision • Termination of Application • Oversight of Grantees • Revocation of Grant • Annual Conformity Review **NOTES**: • the validity period of the Grant shall be set at three years subject to the continued adherence to conformity terms and conditions • where the Grant is conditional, a review schedule shall be set to ensure that the Applicant provides, within the required timescale, adequate grounds for the removal of the conditions, without which the Grant shall lapse at the expiry of that timescale • if the Authoritative Body is *not* the Kantara Initiative ARB then that body shall notify the Kantara Secretariat of the required details of the Grant; • Kantara Initiative shall update the Kantara Trust Status List with details of the new Grantee within two business days.

OBSERVATIONS: Compliance: Kantara Initiative's Assurance Assessment Scheme appears to meet the requirements of BS EN ISO/IEC 17065.

RECOMMENDATIONS: Further investigation by personnel expert in BS EN ISO/IEC 17065 will need to be undertaken to confirm this preliminary finding.

REVISION HISTORY

0.1 March 10, 2015 Initial Draft

1.0 April 8, 2015 Comments from Kantara Initiative and the UK incorporated including a change in the title of the study and the document.