MEMORANDUM OF UNDERSTANDING
BETWEEN

The Kantara Initiative Inc., Delaware, USA (“KI”)

AND

Identity Ecosystem Steering Group, Inc., USA (“IDESG”)

(The Kantara Initiative Inc. and the Identity Ecosystem Steering Group Inc are hereinafter collectively referred to as the “Parties” and individually as a “Party”)

November 1, 2017

Background, Context and Purpose

IDESG and KI are respected members of the personal identity and privacy community that spans a range of like-minded organizations which strive for a fairer and safer identity ecosystem to support the digital economy.

The organizations share much in terms of goals, purpose and intent while maintaining their individual organization's focus. We are all strengthened by unity while maintaining our individual niches, paths and a purpose that differentiates us in pursuit of that 'big picture' greater good.

The organizations have a track record of collaboration. KI was the first organization to enter into a formal Liaison Agreement with IDESG and until this year, was the only Liaison Agreement that IDESG had entered into. IDESG and KI intend to deepen the existing relationship through a collaboration on the organizations' respective identity assurance conformance assessment programs.

Over the past 12 months, IDESG has undertaken a mapping of the IDESG Baseline Requirements confirmed in the Identity Ecosystem Framework (IDEF) to the Kantara Identity Assurance Framework Service Assessment Criteria (SACs) with a view to allowing third-party-assessed, Kantara-approved CSPs and Component providers to be partially conformant to the IDEF by virtue of such approval. This has mutual benefit to both organizations – on the one hand, adding more value to the Kantara scheme for its participants, and on the other, adding more self-attested registrants to the IDEF.

The purpose of this Memorandum of Understanding (MOU) is to formally recognize the concept and operation whereby Approved CSPs and/or Component providers thereof under the Kantara IA Program can be onboarded onto the IDESG self-attested Identity Ecosystem Framework (IDEF) Registry program and trusted as conformant with a declared confirmed subset of the IDEF Baseline Requirements, delisted when compliance in Kantara expires, together with the associated lifecycle management and promotion of the activity to be known as 'the Identity Ecosystem Partnership'.

1. **Goals of the Collaboration**

   The collaboration has the following goals, while maintaining separate and distinct brands for its identity assurance programs:

   - Promote the existence of this MOU to each other's membership and participant bases;

   - Confirm onboarding and delisting processes with Annex 1 to this MOU

- Regularly update and improve the processes and other aspects of the collaboration for IDESG self-attestation and Kantara approval.

- Explore the feasibility of further collaboration on activities currently outside the scope of this MOU, such as future third party assessment of IDESG's IDEF in areas such as outsourcing to Kantara IDESG's program governance, third party assessment, and approval scheme under IDESG's brand.

2. Management and Terms of the Collaboration

a. Principal Point of Contact

For KI:
Ruth Puente
Program Manager,
Kantara Initiative Inc.

ruth@Kantarainitiative.org

For IDESG:
Benjamin T. Wilson
TFTM Committee Chair,
IDESG

ben.wilson@digicert.com

b. Annexes

Attached hereto are Annexes A, B and C (as amended, restated, or otherwise modified from time to time by the Parties). The Parties agree that on a semi-annual basis they will revisit the processes and responsibilities listed in Annex A and modify them to ensure that they are effective and to be implemented. The Parties acknowledge that the Annexes may be modified without the necessity of re-signing this MOU.

3. Consultation and Confidentiality

- The Parties agree that the timely, open, and collaborative exchange of information and consultation is essential to ensure mutual success of the collaboration.

- All (business confidential) information that the Parties exchange within the context of this Memorandum of Understanding will be confidential to the receiving Party and its members and advisors and can only be shared with third parties with prior written approval by the other Party.

- The Parties agree to proactively share any relevant, publicly disclosable developments, news or initiatives that transpire in the e-Identity, security, personal data, and privacy spaces.

4. Costs and Expenses

Each Party will bear its own costs and expenses unless otherwise agreed upon in writing signed by both Parties, with terms of any invoices payable to either Party determined and negotiated by a separate agreement.

5. Publicity

All public notices to third parties and all other publicity concerning this Memorandum of Understanding shall be jointly planned and coordinated by the Parties and neither Party shall act unilaterally in this regard without the prior approval of the other Party (such approval shall not be unreasonably withheld, conditioned or delayed), except where required to do so by law or by the applicable regulations, rules or policies of any governmental or other regulatory agency having jurisdiction in respect of the Party. When seeking the prior approval of the other Party, the Parties will use reasonable efforts, acting in good faith, to agree upon text and imagery/logos for such statement or press release that is satisfactory to both Parties.

6. Acknowledgement and Recognition

Given the mutual exchange of benefits that each Party is providing to each other and to the communities each serves, each Party agrees to ensure the other is appropriately recognized for its contributions to the collaboration, subject to the following, and to the restrictions on written statements and use of text, imagery and logos referred to in 5, above. This recognition may include the following, subject to advance notification and agreement by the Parties prior to any public release:

- Announcement on either Party's website and in a formal press release outlining the agreement between IDESG and KI pertaining to this MOU.

- Ongoing endorsement of the Party via name and/or logo as a participant on relevant and mutually agreed upon collateral such as websites, social media, and in print communication materials, including branding for specific collateral associated with individual projects that emerge from the collaboration, such as program developments, events, and other activities.

- Activities, events, workshops or the like that jointly involve IDESG and KI teams may be written about (as blogs, articles, tweets, etc.) or videotaped and made available as summary content on the IDESG website and the KI website and other related web and social media properties. Either Party's brand will be associated with the content for such materials in the format that is most appropriate (e.g., Twitter handle, logo placements, etc.).

7. Non-Exclusivity

Each Party recognizes that the cooperation envisaged under this Memorandum of Understanding is not exclusive and that neither Party is precluded from entering into any similar arrangement or agreement with any other Party.

8. Reporting

On a quarterly basis, or as otherwise agreed to by the Parties, the Principal Contacts will assess the progress of the collaboration, including any problems, concerns, results, opportunities for continuous improvement, and any other information material to the progress and success of the collaboration.

9. Terms and Termination

This Memorandum of Understanding will come into effect as of the date on the title page, and will remain in force unless terminated earlier by either Party. This Memorandum of Understanding may be amended or renewed upon written approval of the Parties. Either Party may terminate this Memorandum of Understanding upon providing the other Party with sixty (60) days written notice.

In the case that this Memorandum of Understanding is terminated by one of the Parties, the other Party has no right to compensation or any damages whatsoever.

10. Complete Agreement

Except as may be modified as set forth in Section 2.b. above, this MOU contains the Parties' entire legally binding agreement respecting the subject matter hereof and may be modified only by signed written document.

IN WITNESS WHEREOF, the Parties have executed this Memorandum of Understanding as of the Effective Date on the front page of this MOU.

Kantara Initiative, Inc.	**IDESG**
By: ____________________________	By: ____________________________
Name: Colin Wallis	Name Mark DiFraia
Title: Executive Director, KI	Title: President, IDESG
Date: __________________________	Date: __________________________
Phone: +44 (0) 7490 266 778	Phone: +1 646-385-0586
Email: colin@kantarainitiative.org	Email: Mark.DiFraia@us.idemia.com

Annex A:

1. Onboarding Process:

The following 6 steps present the key activities for the on-boarding of Kantara-approved CSPs and Service Components to the IDESG IDEF Registry. These steps are detailed in the sections that follow.

1. Mapping Kantara Initiative IAF 1400 Service Assessment Criteria and related profiles to IDEF Baseline Requirements.
2. Determine and confirm conformance disposition for mapped requirements.
3. Prequalification of Kantara-approved CSPs and Service Components for applicable IDEF Baseline Requirements (based on Steps 1 & 2).
4. Kantara-approved CSPs and Service Components self-assessment and attestation for IDEF Baseline Requirements that are not prequalified.
5. Facilitated application/registration processes for Kantara-approved CSPs and Service Components (using IDESG Concierge Service).
6. Listing on IDEF Registry for Kantara-approved CSPs and Service Components.

Step 1: Mapping Kantara IAF 1400 and Profiles to IDEF Baseline Requirements.

The IDESG developed an Excel workbook that was used as the basis for requirements mapping and comparison for the IDEF Baseline Requirements and Kantara IAF 1400 Service Assessment Criteria and the Kantara U.S. Federal Privacy Profile. Kantara IAF 1400 Service Assessment Criteria were mapped for Kantara Levels of Assurance 2. 3, and 4. The IDESG provided all mapping for all requirements of the Kantara IAF 1400 Service Assessment Criteria and the Kantara U.S. Federal Privacy Profile to the IDEF Baseline Requirements. The requirements mappings were confirmed by Kantara.

Step 2: Conformance disposition for mapped requirements.

The IDESG evaluated all IAF 1400 Service Assessment Criteria that were mapped to the IDEF in Step 1 for conformance to the performance outcomes of the IDEF Baseline Requirements. The same conformance evaluation was performed for the Kantara U.S. Federal Privacy Profile. Conformance dispositions were determined based on the following status: F=Full, P=Partial, NE=Not Equivalent, NCR=No Comparable Requirement, N/A=Not Applicable. In circumstances where multiple IAF 1400 SACs were mapped to a single IDEF Baseline Requirement, the combination of SACs in total were assessed to determine conformance to the Baseline Requirement. The conformance dispositions for the IAF 1400 and the U.S. Federal Privacy Profile were confirmed by Kantara.

Step 3: Prequalification of Kantara-approved CSPs and Service Components for applicable IDEF Baseline Requirements.

Kantara-approved CSPs and Service Components are provided the following prequalification status for applicable IDEF Baseline Requirements:

- "Fully Implemented" status for Kantara certifications at LOA 2, 3, and 4 for Baseline Requirements mapped "F" for "Full" conformance.
- "Implementation Underway" for Kantara certifications at LOA 2, 3, 4 for Baseline Requirements mapped with "P" for "Partial Conformance".
- No prequalification for Baseline Requirements mapped with "NCR" for "No Comparable Requirement" or "NE" for "Not Equivalent".
- Baseline Requirements with "N/A" for "Not Applicable" status are not applicable to the CSPs or Service Components.

The prequalification status for Kantara-approved Credential Service Providers (CSPs) and Service Components is presented in Annex B.

Step 4: Kantara-approved CSPs and Service Components self-assessment and attestation for IDEF Baseline Requirements that are not prequalified.

To be listed on the IDEF Registry, Kantara-approved CSPs and Service Components will need to self-assess and attest to the implementation status for all applicable IDEF Baseline requirements for which they are not prequalified as "Fully Implemented" or "Not Applicable".

Step 5: Facilitated application/registration processes for Kantara-approved CSPs and Service Components (using IDESG Concierge Service).

To be listed on the IDEF Registry, Kantara-approved CSPs and Service Components will need to register and apply to the IDESG. The IDESG Concierge Service will facilitate the registration and application process for these applicants.

Step 6: Listing on IDEF Registry for Kantara-approved CSPs and Service Components.

The IDESG will list all Kantara-approved CSPs and Service Components that complete the application/registration step on the IDEF Registry. The listings for these CSPs and Service Components will be annotated to show that they are Kantara approved and will include a link to their Kantara certification.

Step 7: Ongoing Maintenance

On an ongoing basis, both IDESG and KI will monitor changes to their listing criteria and repeat Steps 1 through 6 as necessary.

2. De-Listing Process

Kantara-approved CSPs and Service Components will continue to be listed on the IDESG IDEF Registry provided they comply with the IDEF Registry Terms of Use and continue to be certified as a Kantara-approved CSP or Service Component. Any question of noncompliance with the IDEF Terms of Use are subject to the notification and corrective action requirements of the IDEF Registry Terms of Use. If, for any reason, the Kantara-approved CSPs and Service Components no longer maintain their Kantara-approved certification, the CSPs and Service Components will be notified that a new application and attestation will be required in order to continue their listing on the IDESG Registry. The new application will require that the CSPs and Service Components assess and attest to the implementation status of the previously prequalified IDEF Baseline Requirements that were based on their Kantara certification. The annotation for Kantara certification and link to Kantara certification will be removed from the IDEF Registry listing. Failure to timely re-apply to the IDEF Registry following Kantara de-certification will result in removal of the listing from the IDEF Registry.

Any listed organization may voluntarily request de-listing and removal from the IDEF Registry at any time.

3. IDESG Responsibilities

a. Map Kantara Initiative Service Assessment Criteria and related profiles to IDEF Baseline Requirements.
b. Grant, in accordance with Step 3 and Annex B, pre-qualification status to Kantara-approved Credential Service Providers (CSPs) and Service Components.
c. Maintain publicly accessible web pages showing the Annex 2 mapping of the IDEF to Kantara SACs showing which requirements are met by virtue of Kantara third party assessment: one page for approvals of full-service CSPs at LoAs 2 and 3, one page for approvals of full-service CSPs using the Kantara Federal Privacy profile, one page for Kantara Credential Management component approvals, and one page for Kantara Identity Proofing component approvals.
d. Put an automated watch on, and regularly visit, the Kantara Registry webpage to determine then-current CSP status.
e. Reach out to the CSP/component service contact shown on the Kantara Registry webpage (or asks the Kantara Program Manager for contact details).
f. Determine new potential participants for the IDESG IDEF Registry program, with the requisite web page link/s applicable to their highest approved LoA level and the Privacy Profile.
g. Provide written guidance and other support (e.g. a concierge) to Applicants to facilitate the registration and application process.
h. List all Kantara-approved CSPs and Service Components that complete the application/registration process on the IDEF Registry and provide a link to the Kantara Registry webpage.

i. Advise KI of changes to the IDESG's IDEF requirements.

4. KI Responsibilities

a. Review mapping of Kantara SAC and profiles to IDEF Baseline Requirements and determine and confirm/reject conformance disposition for mapped requirements.
b. Maintain the Kantara Registry webpage to show the then-current status of CSPs and Component Services (both new additions and removed/withdrawn approved CSPs and Component services).
c. Implement a script that sends notifications when there are status changes on the Kantara Registry webpage's Status list.
d. Email or otherwise confirm with the IDESG IDEF Registry Program Manager of status changes on the Kantara Registry webpage. However, this process is not dependent on such email.
e. Advise IDESG of any changes to the Kantara SAC and other profiles.

5. Kantara-approved CSP and Service Component Responsibilities

a. Register with / apply to the IDESG for listing in the IDEF Registry.
b. Comply with the IDEF Registry's Terms of Use (General Terms of Use and Supplemental Terms of Use).
c. Self-assess and attest to the implementation status for all applicable IDEF Baseline requirements for which they are not prequalified as "Fully Implemented" or "Not Applicable".

…….

Annex B

Annex B shows the confirmed conformance disposition for all IDESG IDEF Baseline Requirements based on the mapping of Kantara IAF 1400 and the Kantara U.S. Privacy Profile to those requirements. Table 1 displays the conformance disposition for all IDEF Baseline Requirements and will be applied to Kantara-approved (full service) Credential Service Providers.

Table 1: Confirmed IDEF and IAF 1400 SAC Conformance Disposition
IAF 1400 SAC

IDEF Baseline Requirement	Conformance Disposition	IDEF Baseline Requirement	Conformance Disposition	IDEF Baseline Requirement	Conformance Disposition
INTEROP-1	NCR/NA	PRIVACY-8	P	SECURE-8	F
INTEROP-2	LOA 4: P, LOA 2,3: NCR	PRIVACY-9	P	SECURE-9	F
INTEROP-3	LOA 4: P LOA 2,3: NCR	PRIVACY-10	NCR	SECURE-10	F
INTEROP-4	LOA 4: P LOA 2,3: NCR	PRIVACY-11	NCR	SECURE-11	F
INTEROP-5	F	PRIVACY-12	NE	SECURE-12	F
INTEROP-6	F	PRIVACY-13	NCR	SECURE-13	F
INTEROP-7	NCR	PRIVACY-14	P	SECURE-14	F
INTEROP-8	F	PRIVACY-15	NE	SECURE-15	F
PRIVACY-1	P	SECURE-1	F	USABLE-1	NCR
PRIVACY-2	NCR	SECURE-2	F	USABLE-2	NCR
PRIVACY-3	NCR	SECURE-3	F	USABLE-3	NCR
PRIVACY-4	NCR	SECURE-4	F	USABLE-4	NCR
PRIVACY-5	NCR	SECURE-5	F	USABLE-5	NCR
PRIVACY-6	P	SECURE-6	F	USABLE-6	NCR
PRIVACY-7	F	SECURE-7	F	USABLE-7	NCR

Table 2: Confirmed IDEF and Kantara U.S. Federal Privacy Profile Conformance Disposition

IDEF Baseline Requirement	Conformance Disposition	Baseline Requirement	Conformance Disposition	Baseline Requirement	Conformance Disposition
PRIVACY-1	F	PRIVACY-7	F	PRIVACY-13	P
PRIVACY-2	F	PRIVACY-8	P	PRIVACY-14	F
PRIVACY-3	P	PRIVACY-9	F	PRIVACY-15	NE
PRIVACY-4	NCR	PRIVACY-10	F	INTEROP-4	F
PRIVACY-5	F	PRIVACY-11	F	INTEROP-7	F
PRIVACY-6	F	PRIVACY-12	P	INTEROP-8	F

Annex C

Kantara-Approved (full service) CSPs Prequalification for IDEF Baseline Requirements

Kantara-approved Credential Service Providers offer the full scope of services covered by IAF 1400 and are assessed against all the applicable Service Assessment Criteria. Therefore, the full scope of IDEF Baseline Requirements conformance disposition from Annex B Table 1 apply to Kantara-approved Credential Service Providers. This prequalification is displayed in Table 3 below.

Table 3: IDEF Registry Prequalification for IDEF Baseline Requirements for Kantara-approved CSP (full service)

IDEF Baseline Requirement	Conformance Disposition	IDEF Baseline Requirement and Registry Prequalified Implementation Status
INTEROP-2	LOA 4: P LOA 2,3: NCR	LOA 4: Implementation Underway LOA 2,3: None
INTEROP-3	LOA 4: P LOA 2,3: NCR	LOA 4: Implementation Underway LOA 2,3: None
INTEROP-4	LOA 4: P LOA 2,3: NCR	LOA 4: Implementation Underway LOA 2,3: None
INTEROP-5	F	Fully Implemented
INTEROP-6	F	Fully Implemented
INTEROP-8	F	Fully Implemented
SECURE-1	F	Fully Implemented
SECURE-2	F	Fully Implemented
SECURE-3	F	Fully Implemented
SECURE-4	F	Fully Implemented
SECURE-5	F	Fully Implemented
SECURE-6	F	Fully Implemented
SECURE-7	F	Fully Implemented
SECURE-8	F	Fully Implemented
SECURE-9	F	Fully Implemented
SECURE-10	F	Fully Implemented
SECURE-11	F	Fully Implemented
SECURE-12	F	Fully Implemented
SECURE-13	F	Fully Implemented
SECURE-14	F	Fully Implemented
SECURE-15	F	Fully Implemented
PRIVACY-1	P	Implementation Underway
PRIVACY-6	P	Implementation Underway
PRIVACY-7	F	Fully Implemented
PRIVACY-8	P	Implementation Underway
PRIVACY-9	P	Implementation Underway
PRIVACY-14	P	Implementation Underway

Table 4: IDEF Registry Prequalification for IDEF Baseline Requirements for Kantara Approvals for Kantara U.S. Federal Privacy Profile

IDEF Baseline Requirement	Conformance Disposition	IDEF Baseline Requirement and Registry Prequalified Implementation Status
PRIVACY-1	F	Fully Implemented
PRIVACY-2	F	Fully Implemented
PRIVACY-3	P	Implementation Underway
PRIVACY-5	F	Fully Implemented
PRIVACY-6	F	Fully Implemented
PRIVACY-7	F	Fully Implemented
PRIVACY-8	P	Implementation Underway
PRIVACY-9	F	Fully Implemented
PRIVACY-10	F	Fully Implemented
PRIVACY-11	F	Fully Implemented
PRIVACY-12	P	Implementation Underway
PRIVACY-13	P	Implementation Underway
PRIVACY-14	F	Fully Implemented
INTEROP-7	F	Fully Implemented
INTEROP-8	F	Fully Implemented

Kantara-approved Service Components

In addition to approving full service Credential Service Providers, the Kantara Initiative also provides approval for Service Components that offer only part of the full services of Credential Service Providers. Service Components may be approved as Identity Proofing and Verification Service Component Providers or Credential Management Component Service Providers. As Service Components, all the IAF 1400 Service Assessment Criteria may not be included in the scope of Assessments performed by Kantara-certified Assessors. Based on the IAF 1400 and IDEF mapping, Tables 5 and 6 show the IDEF Registry Baseline Requirements prequalification for Kantara-approved Component Service Providers.

Table 5: IDEF Registry Prequalification for IDEF Baseline Requirements for Kantara-approved Identity Proofing and Verification Service Component Providers

IDEF Baseline Requirement	Conformance Disposition	IDEF Baseline Requirement and Registry Prequalified Implementation Status
INTEROP-5	F	Fully Implemented
INTEROP-6	F	Fully Implemented
INTEROP-8	F	Fully Implemented
SECURE-1	F	Fully Implemented
SECURE-2	F	Fully Implemented
SECURE-5	F	Fully Implemented
SECURE-6	F	Fully Implemented
SECURE-8	F	Fully Implemented
SECURE-9	F	Fully Implemented
SECURE-10	F	Fully Implemented
SECURE-14	F	Fully Implemented
SECURE-15	F	Fully Implemented
PRIVACY-1	P	Implementation Underway
PRIVACY-6	P	Implementation Underway
PRIVACY-7	F	Fully Implemented
PRIVACY-8	P	Implementation Underway
PRIVACY-9	P	Implementation Underway
PRIVACY-14	P	Implementation Underway

Table 6: IDEF Registry Prequalification for IDEF Baseline Requirements for Kantara-approved Credential Management Component Service Providers

IDEF Baseline Requirement	Conformance Disposition	IDEF Baseline Requirement and Registry Prequalified Implementation Status
INTEROP-2	LOA 4: P LOA 2,3: NCR	LOA 4: Implementation Underway LOA 2,3: None
INTEROP-3	LOA 4: P LOA 2,3: NCR	LOA 4: Implementation Underway LOA 2,3: None
INTEROP-4	LOA 4: P LOA 2,3: NCR	LOA 4: Implementation Underway LOA 2,3: None
INTEROP-5	F	Fully Implemented
INTEROP-6	F	Fully Implemented
INTEROP-8	F	Fully Implemented
SECURE-1	F	Fully Implemented
SECURE-2	F	Fully Implemented
SECURE-3	F	Fully Implemented
SECURE-4	F	Fully Implemented
SECURE-5	F	Fully Implemented
SECURE-6	F	Fully Implemented
SECURE-7	F	Fully Implemented
SECURE-8	F	Fully Implemented
SECURE-9	F	Fully Implemented
SECURE-10	F	Fully Implemented
SECURE-11	F	Fully Implemented
SECURE-12	F	Fully Implemented
SECURE-13	F	Fully Implemented
SECURE-14	F	Fully Implemented
SECURE-15	F	Fully Implemented
PRIVACY-1	P	Implementation Underway
PRIVACY-6	P	Implementation Underway
PRIVACY-7	F	Fully Implemented
PRIVACY-8	P	Implementation Underway
PRIVACY-9	P	Implementation Underway
PRIVACY-14	P	Implementation Underway