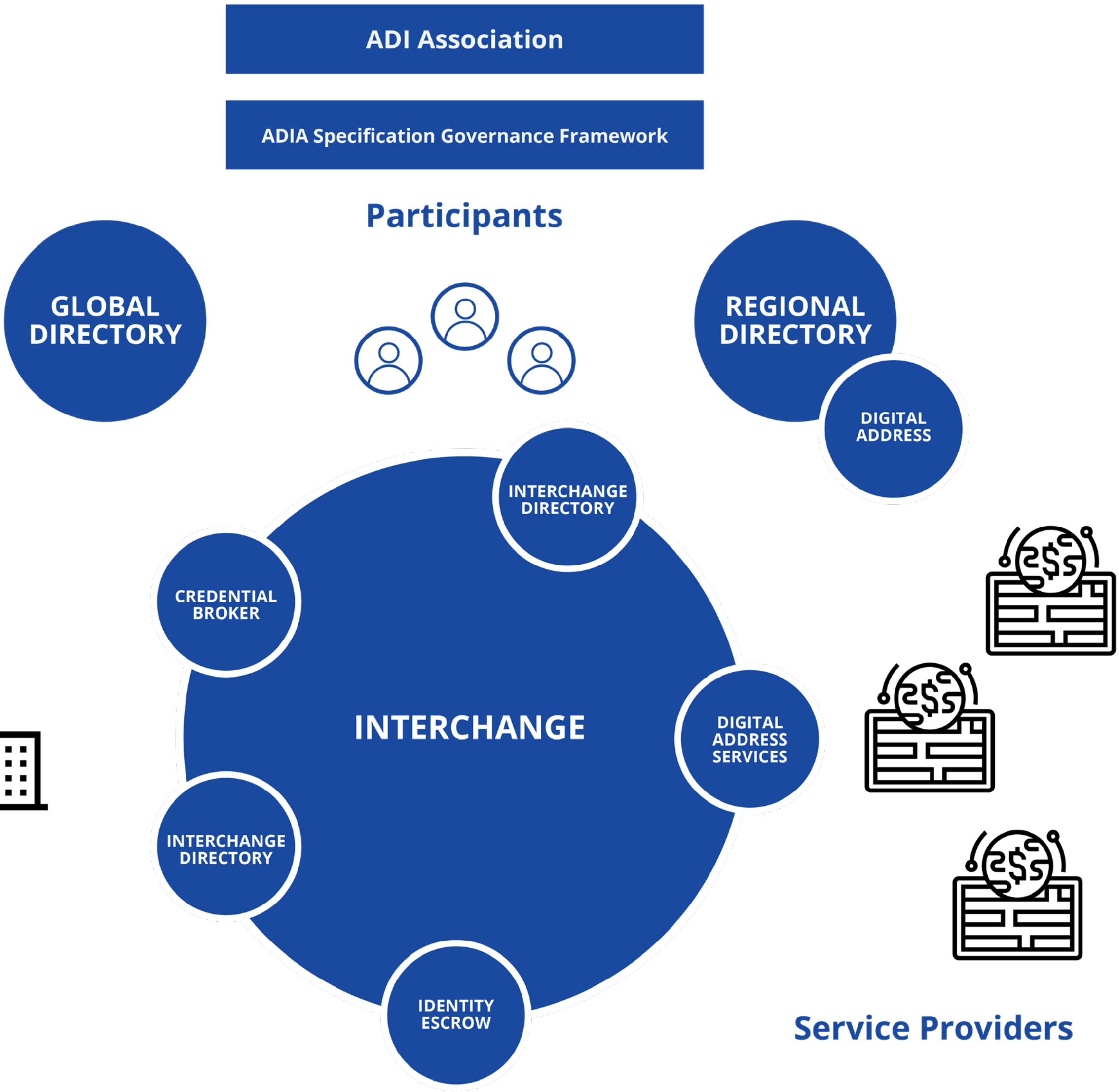
Accountable Digital Identity | ADI Association

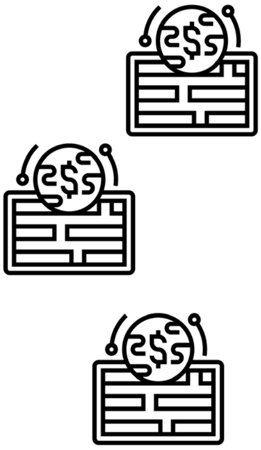
Trust through accountable, privacy-preserving digital identity

Specification Governance

Version 2.1

THE ADIA ECOSYSTEM





THE ADIA ECOSYSTEM

The Accountable Digital Identity Association

The ADI Association is a 501c3 nonprofit that brings companies and organizations together to advance and scale easy-to-use verifiable identity and data credentials through the ADIA Specification, a combination of processes, protocols, services, and their associated governance that enables privacy-preserving, accountable digital identity.

The ADI Association is responsible for establishing and administering the governance of the ADIA Specification and its component services, as specified by this and any related governance document, including all legal agreements.

ADIA Specification Governance Framework

The ADIA Specification Governance Framework (this document and all related procedural documents, guidelines and legal agreements), form the controlled documents for governing the ADIA Specification. The Board of the ADI Association is responsible for approving, implementing, and updating the Specification Governance Framework.

Issuers

Issuers are organizations that are vetted and on-boarded into the ADIA ecosystem to issue identity claims to end Participants by participating in an Interchange. These could be healthcare providers, employers, educational institutions, government agencies, and others that meet the ADI Association's Assurance Guidelines for onboarding Issuers into the ecosystem and become members of the ADI Association.

Participants

Participants are the people who receive verifiable identity credentials and digital addresses. They obtain verifiable credentials from Issuers, as needed, and can use them at their own discretion without a centralized authority managing, monitoring, or using their identity data without consent.

Participants are assured they control their identity with strong authentication, provided by tools such as Fido.

Participants can use verifiable credentials in the ADIA ecosystem with or without data enabled mobile devices. In all cases, they can be assured that sharing information is secure and by consent only, with the addition of strong authentication tools such as FIDO or other strong authentication processes between the participant and the interchange. The ADIA Specification provides user privacy as a core principle.

Service Providers

Service Providers are those entiities who verify digital credentials within the ADIA Specification in order to deliver services to Participants through Interchanges. They can ascertain the trustworthiness of the Issuer by verifying the identity data presented by the Participant.

Global Directory

The Global Directory contains an index of Issuers, Service Providers, and Interchange Services in the ADIA ecosystem. Global Directory Service operators must be board members of the ADI Association.

When an entity is onboarded, it is added to the Global Directory as an Issuer or Service Provider or Interchange Service. Once listed, it can be located by individuals or other entities and services. If an entity leaves the ADI Association, it will be delisted from the Global Directory.

Regional Directories

Regional Directories are primarily a way to identify and connect with Participants, i.e., end users, in an Interchange. Each Interchange must be associated with one Regional Directory. Participants must be able to request delisting from a Directory.

Interchange

The Interchange is a collection of services provided by Interchange Providers.

Interchange Provider

An Interchange Provider is a company that provides one or more interoperable services in an Interchange as defined by the ADIA Specification that enable the use of verifiable identity and data credentials in multiple contexts.

The Digital Address (DAS)

A digital address is a simple way for a person to access a verifiable digital credential and prove who they are online. It enables access to the ADIA ecosystem both for people with smart devices as well as those who do not have access to computers or smartphones.

Digital Addresses are non-correlating across multiple issuers or verifiers and only lead the verifier to the specific information the Participant has approved them to access.

Digital addresses are composed of a short, easy-to-remember word or phrase that acts as a pointer to the Interchange Service Provider that will conduct a specific identity action. The address has a prefix such as Jane007 and a suffix containing the home Digital Address Service, such as @mrvl.

It's important to note that in the ADIA ecosystem a Digital Address is an alias for a unique identifier; it is not the unique identifier.

The Digital Address Service

Digital Address Services (DAS) enable identity transactions to occur in the ADIA ecosystem by providing a cloud-hosted agent that communicates with Issuers, Service Providers, Directories, and other services on behalf of the Participant.

All Participants have a Digital Address Service; some issuers and service providers have agents hosted at an Interchange Provider too. All communication in these interactions uses DIDcomm protocols.

Each Participant's DAS holds cryptographic keys and verifiable digital credentials on behalf of the Participant. The DAS maintains the Participant's directory listings and requests for unique DIDs when a new connection is made. All communication in these interactions uses DIDcomm protocols.

The DAS is configured for and uses machine-readable governance framework documents as policy for automatically accepting or rejecting verifiable credential interactions. When necessary, the DAS will communicate with the Participant through a secure channel and obtain consent. When consent is required, Participants authenticate themselves to the Agent through FIDO.

All interactions through the agent are logged by the agent and available for inspection by the Participant.

Identity Escrow

Identity Escrow enables privacy-preserving accountability, a key feature of the ADI ecosystem. For high-value or high-risk interactions, Participants can consent to their identity being placed in escrow as a way to enable accountability should they violate the terms or service set by the Issuer of the verifiable credential.

Identity data is presented to the Identity Escrow Service in a verifiable credential from an approved Issuer. The Escrow Service stores the data and issues a verifiable escrow credential to the Participant. Each verifiable escrow credential obtained by the Participant contains a unique id.

Upon connecting to a new Service Provider, the Participant presents the verifiable escrow credential. The Service Provider validates the verifiable escrow credential and retains the unique id. Should the Participant violate the terms of service or otherwise require accountability for their actions, the Service Provider will present the request and corresponding evidence to the Escrow Service. The Escrow Service will evaluate the request and evidence against their policies. If policy indicates, the Escrow Service will notify the Participant of the disclosure, disclose the identity data from escrow, and log the evidence and disclosure for independent audit. Disclosure logs are retained for a period set by policy.

Both the Service Provider and the Participant must agree on the terms and policy of the Identity Escrow Service. The right to be forgotten may be delayed for a period of time to allow adequate time for violation disclosure requests to be processed and resolved.

Credential Broker

A Credential Broker facilitates the exchange and presentation of verifiable credentials between Issuers, Participants, and Service Providers. It also resolves differences in verifiable credential formats and can enable payments between parties and resolve payment system differences.

Interchange Directories

Interchange Directories are a way to identify and connect with Participants through a particular scope, which can be geopolitical, like a country, or organizational, such as a multi-national medical organization, or a university. Interchange Directories are not hosted on a ledger as participants must be able to request delisting from a Directory.

1. ADIA Specification Policies

1.1 The ADIA Specification is an interoperable specification for accountable, privacy-preserving digital identity through the use of distributed and secure verifiable credentials and decentralized identifiers, and related services.

1.2 The ADIA Specification is governed by the policies contained within this controlled document, The ADIA Specification Governance Framework, and administered by the ADI Association Board of Directors and its Officers.

1.3 The ADIA Specification Governance Framework is composed of the policies, procedures, guidelines, and legal agreements for the ADIA Specification and, as a series of living documents, the Framework will be, periodically,updated by the Board of Directors of the ADI Association in line with the Association's mission and values.

1.4 The Specification Framework consists of the following:

2. Policies on Protocols and Standards

2.1 The ADIA Specification is governed by ADI Association

2.2 The ADIA Specification follows the W3C Verifiable Credentials Data Model and the DID Specification as governed by the W3C Credentials Community Group.

2.3 The ADIA Specification references the Hyperledger Aries DIDcomm V1 specification as specified in the appropriate Aries RFC.

2.4 The ADIA Specification follows relevant Hyperledger Aries specifications as specified in the appropriate Aries RFC.

2.5 For further details, see the Accountable Digital Identity Association (ADIA) Specification.

3. Policies on Privacy

3.1 The ADI Association will work with external, regional experts to ensure compliance with all relevant jurisdictional data privacy regulations, including the European Union's General Data Protection Regulation (GDPR), the California Consumer Protection Act (CCPA), and Brazil's Lei Geral de Proteção de Dados Pessoais (LGPDP).

3.2 The ADI Association will, under expert guidance, continuously update its privacy policies to reflect regional changes in privacy law.

3.3 For ADI Association members engaged in business with the EU, the roles and obligations with respect to Data Control and Data Processing under GDPR are set out in the ADIA Data Privacy Agreement (DPA).

3.4 Where the ADI Association enters into a Data Processing Agreement, the Association will audit for GDPR compliance through quarterly internal audits.

4. Policies on Security

4.1 All Interchanges and Interchange Service Providers MUST maintain and follow IT security policies and practices that are integral to maintaining and protecting the privacy and security of Issuers, Services and Participants in the ADIA ecosystem.

4.2 The ADI Association recommends Issuers, Interchanges, Interchange Service Providers and Service Providers following the standards for meeting SOC1 and SOC2 audit, and the zero trust model for network security.

4.3 The ADI Association will periodically request third-party security audits of the operations of Interchange and Interchange Service Providers.

4.4 The ADI Association will periodically request third-party security reviews from the interchanges for compliance with the ADI Specification architecture.

5. Policies on Compliance

5.1 The ADI Association follows US, UK, and EU AML laws. For further details, see ADIA's AML document.

6. Policies on Documents

6.1 This governance document and ADI Association documents linked to this document are all controlled documents.

7. Policies on Interchanges

The purpose of an Interchange is to serve the ADIA ecosystem by vetting, approving, and managing Issuers, Service Providers, Interchange-level directories, Digital Address Services, Identity Escrow Services, and Brokerage Services.

7.1 To create an Interchange, a company MUST be approved for membership of the ADI Association and, upon approval, then apply for and pass certification as an Interchange by the ADI Association.

7.2 To be certified, Interchanges MUST be functionally compliant with the ADIA Specification, and pass the interoperability and Digital Address Service-to-Digital Address Service communication tests that are specified in the certification process.

7.3 Interchanges MUST also agree to follow the governance policies for vetting and onboarding Issuers, Participants, Service Providers, Agent Custodial Services, Credential Brokers, and Identity Escrow Services as specified in the governance policies of the ADIA Specification (this document), Regional governance policies, and the ADIA Guidelines on Assurance.

8. Policies on Issuers

Issuers are organizations that are vetted and on-boarded into the ADIA ecosystem to issue identity claims to Participants by participating in an Interchange.

8.1 Companies and organizations that want to issue verifiable credentials (Issuers) using the ADIA Specification MUST apply for membership to the ADI Association through an Interchange Provider within a region. Interchange Providers are companies that provide the technology for Issuers, Service Providers, Brokers and other associated services.

8.2 The Interchange provider MUST conduct the vetting of the Issuer based on ADIA's Guidelines on Assurance and submit a membership application to ADIA on the Issuer's behalf. Applications are reviewed by the Membership Committee of the ADI Association board.

8.3 Annual membership is subject to meeting the assurance criteria set out in the application, signing the issuer agreement, complying with audit requirements, and paying the annual ADI Association membership fees.

8.4 Applications MUST be processed on a regional basis, with application criteria normed to the best assurance practices for that region. Regions MUST set out assurance levels for Issuers and verifiable credentials following the ADI Association's Guidelines on Assurance (see also Policies on Regions).

8.5 An Issuer MUST agree to the assurance criteria for issuing verifiable credentials to Participants as outlined in the ADI Association Application, ADI Association Agreement, and as specified in the ADI Association Guidelines on Assurance.

8.6 All Issuer members of the ADI Association will be subject to a review and annual renewal fee as a requirement to retain standing as an issuer. The review is performed by the Membership Committee of the ADI Association. If the Issuer membership is not renewed, the verifiable credential will be managed as per section 10.

8.7 Violation of ADI Association Policies on Verifiable Credentials and Issuance as stated within this governance framework MAY result in suspension and/or non-renewal of the Issuer's Association membership.

8.8 If an Issuer exits the ecosystem, the verifiable credentials it issued will be either transferred to a new storage location or invalidated. The course of action will depend on the reasons the Issuer exited the ecosystem and the viability of the previously issued verifiable credentials. These will be assessed by their respective Interchange with oversight by the ADI Association.

9. Policies on Service Providers

Service Providers are those entities who verify digital credentials within the ADIA Specification in order to deliver services to Participants through Interchanges.

9.1 Companies and organizations that want to verify verifiable credentials (Service Providers) using the ADIA Specification MUST apply for membership of ADI Association through an Interchange Provider within a region. Interchange Providers are companies that provide the technology for Issuers, Service Providers, Brokers, and other associated services.

9.2 The Interchange provider MUST conduct the vetting of the Service Provider based on its legal, tax, and business standing in the region they belong to, and submit a membership application to ADIA on the Service Provider's behalf. Applications are reviewed by the Membership Committee of the ADI Association board.

9.3 Annual membership is subject to meeting the assurance criteria set out in the application, signing the Service Provider agreement, complying with audit requirements, and paying the annual ADI Association membership fees.

9.4 Applications MUST be processed on a regional basis, with application criteria normalized to the best assurance practices for that region.

9.5 All Service Provider members of the ADI Association will be subject to a review and annual renewal fee as a requirement to retain standing as a Service Provider. The review is performed by the Membership Committee of the ADI Association or an ADI Association designated third- party audit service

9.6 Violation of ADI Association Policies on Verifiable Credentials as stated within this governance framework MAY result in suspension and/or non-renewal of the Service Provider's Association membership.

10. Policies on Verifiable Credentials

The purpose of a verifiable digital credential is to enable the attestation and verification of claims about identity in a way that enables consent and ensures privacy.

10.1 Issuers MUST issue verifiable credentials using standard schemas as prescribed by the Interchange Provider where possible, following the technical standards for verifiable credentials and verifiable credential schemas set by the W3C, and as specified by the ADI Association.

10.2 An Issuer MUST reissue a verifiable credential if there is a collision between the hashed attributes for a new listing in a Regional Directory and existing hashed attributes in the Regional Directory, the Issuer MUST resolve this. In the case of disputes, the Directory MUST undertake dispute resolution.

10.3 Verifiable credentials MAY be stored in one of three locations:

a) retained by the Issuer on premise
b) retained by the Issuer in the cloud
c) delivered to the custodial agent of the holder

10.4 Issuers MUST abide by the appropriate data retention policies as established by their Interchange Provider and publish their compliance with these policies. The data retention policies will be established by Interchange Provider while referring to the relevant data protection regulation of the related region.

10.5 Issuers MAY revoke verifiable credentials (e.g., in a situation where an error has been identified in the verifiable credential or the verifiable credential is no longer valid). If they do so, they MUST notify the Participant who holds the verifiable credential. If the Participant has used that verifiable credential for listing in a Regional Directory or Identity Escrow Service, the Participant's Cloud Agent MUST notify the Directory or the Escrow Service of the revocation.

11. Policies on Digital Address Services (DAS)

Digital Address Services (DAS) are part of the services offered by an Interchange. They provide a cloud hosted agent that communicates using DIDcomm protocols with Issuers, Service Providers, Regional Directories, and other services on behalf of the Participant.

11.1 To become a Digital Address Service in the ADIA ecosystem, a company MUST apply to and be approved by an Interchange. A DAS may only be affiliated with a single Interchange.

11.2 The DAS has a fiduciary responsibility to the Participant.

11.3 The DAS MUST only act on behalf of the Participant by consent at the time of the action or if there has been pre-consent as a point of standing policy.

11.4 Strong authentication MUST always be used; FIDO is recommended.

11.5 The DAS MUST have a policy for logging action on behalf of the Participant. Such logging MUST be conducted in accordance with applicable data privacy regulations.

11.6 The Participant MUST be able to review their consent to actions made by the DAS on their behalf.

11.7 Any private keys in use by the Digital Address Services MUST never be shared.

11.8 Annual key rotation is recommended.

12. Policies on Digital Addresses

The purpose of the Digital Address is to function as an alias that allows Participants to easily interact with the ADIA ecosystem and to be looked up within that system.

12.1 A Digital Address MUST uniquely resolve to a DAS and a Participant.

12.2 The Participant MUST create, approve, and register a Digital Address through the Issuer to the DAS.

12.3 The Digital Address SHOULD NOT contain personal identifying information (PII).

12.4 After resolution by the Issuer or Service Provider, the Digital Address MUST NOT be stored or used to extract any further information about the Participant/Entity

12.5 A Participant MUST NOT have more than one digital address per Regional Directory.

12.6 A Participant MAY request that their Digital Address is delisted from a Regional Directory. When a participant is delisted from a regional directory, their digital address and digital identity are completely removed.

12.7 Services and devices MAY register for Digital Addresses.

12.8 Details are available in the Accountable Digital Identity Association (ADIA) Specification and the ADIA Guidelines on Assurance.

13. Policies on the Global Directory

The purpose of the Global Directory is to provide an index of Issuers, Service Providers, and Interchange Services in the ADIA ecosystem.

13.1 13.1 The Global Directory Service operator MUST be a board member of the ADI Association.

14. Policies on Regional Directories

The purpose of a Regional Directory is to connect with Participants or Services in the ADIA ecosystem and to guarantee their uniqueness. Each Interchange MUST be associated with a single Regional Directory. If there are multiple Interchanges in a region, each will have the same Regional Directory to guarantee Participant uniqueness for that Region. There may also be Interchange-level directories that have a specific scope, defined as a logical grouping of Participants according to organization membership, interest, association, or geopolitical similarity.

14.1 To create or operate a Regional Directory, an organization MUST be a board member or sponsor member of the ADI Association.

14.2 A Participant MAY enroll in a Regional Directory upon being issued a verifiable credential with hashed attributes from an approved Issuer. If the participant chooses not to enroll in the regional directory, they do not participate in the ADIA ecosystem.

14.3 The Regional Directory MUST certify that the Issuer is in the ADI Association's list of trusted Issuers and MUST check for any collisions with other hashed attributes before storing the hashed attribute contained in the verifiable credential.

14.4 In the instance of a hash collision (i.e., hashed attributes collide with an existing Participant in a directory), the regional directory MUST reject the registration. The rejected Participant MAY request an investigation by the Regional Directory governance authority to determine the uniqueness of the Participant.

14.5 By consenting to being listed in a Regional Directory, a Participant MUST consent to being looked up in that particular Regional Directory.

14.6 Unique Participant DIDs MUST be generated by the Cloud Agent at the Interchange when a Participant is listed in a Regional Directory.

14.7 Participants MAY request that they be delisted from a Regional Directory in accordance with their local data privacy laws. When a participant is delisted from a regional directory, their digital address and digital identity are completely removed.

14.8 For high-value or high-risk interactions, Participants can also consent to their identity being placed in Identity Escrow to enable accountability should they violate the terms or service set by the Issuer of the credential. The right to be forgotten may be delayed for a period of time to allow adequate time for violation disclosure requests to be processed and resolved.

14.9 A Regional Directory MUST comply with a valid delisting request in accordance with local and jurisdictional data retention policies. The process of deleting a user is explained in the Accountable Digital Identity Association (ADIA) Specification. Interchanges must follow those guidelines.

14.10 A Regional Directory MUST log all delisting requests.

14. Policies on Regional Directories

14.11 The ADI Association MUST periodically audit Regional Directories for compliance with delisting requests, log retention policies, and security policies as per local regulation requirements. This MAY be done directly or or delegated to a third-party auditor.

14.12 In the event that a Regional Directory operator exits the ADIA ecosystem, the Regional Directory information MAY be migrated to a new regional directory operator.

15. Policies on Identity Escrow Services

The purpose of Identity Escrow is to provide consent-based and privacy preserving accountability for policy violations.

15.1 An Identity Escrow Service MUST be onboarded by an Interchange.

15.2 The scope of an Identity Escrow Service is limited to a Regional Directory. Zero or more Identity Escrow Services are allowed within a Regional Directory.

15.3 Participants MAY use any Identity Escrow Service within a Regional Directory.

15.4 Service Providers can use any Identity Escrow Service across any Interchange.

15.5 An issued Escrow identity MUST be unique to avoid correlation without disclosure.

15.6 The terms of service for each instance of Identity Escrow and what constitutes a violation of the terms MUST be made explicit by the Identity Escrow Service and define the information that MUST be placed in escrow and the conditions where that information MUST be released.

15.7 Upon meeting the Participant-consented criteria for identity disclosure, the Identity Escrow Service MUST:

a) reveal the identity of the Participant to the Service Provider
b) notify the Participant of the disclosure event
c) log the disclosure event and the justification for disclosure for independent audit.

The Protocol MUST also inform the

d) Service Provider and the Participant's Cloud Agent.

15.8 The Identity Escrow Service MUST NOT reveal the Participant's identity outside the terms of escrow.

15.9 To become an Identity Escrow Service in the ADIA ecosystem, a company MUST apply through an Interchange Provider. Identity Escrow Services MAY operate across the ADIA ecosystem and are not restricted to a single Interchange. There can be multiple Identity Escrow Services.

15.10 Identity Escrow Services MUST follow local data retention laws.

15.11 If an Identity Escrow Service exits the ADIA ecosystem while escrow contracts are still in effect, they MUST close their account at the Service Provider, and all primary and secondary material related to participants in escrow MUST be destroyed.

15.12 All Identity Escrow Services are subject to annual audit by the ADI Association through a third-party audit service.

16. Policies on Interchange Directories

The purpose of an Interchange Directory is to provide a more flexible, consent-based way to identify people and groups that is distinct from the essential role of a Regional Directory in establishing a unique identification for a Participant within an Interchange; for example, a university or association could run an Interchange Directory for graduates or members. Interchange Directories do not supplant the role of the Regional Directory.

16.1 Organizations or companies wishing to create an Interchange Directory must apply to an Interchange for approval.

16.2 Verifiable credential-based or self-attested attributes CAN be used to list Participants in an Interchange Directory as determined by the Interchange Directory.

16.3 Directories MAY determine their own permissions, public or private.

16.4 A Participant MAY enroll in an Interchange Directory.

16.5 If a Participant opts to be listed in an Interchange Directory, the Participant MUST consent to being looked up in the Interchange Directory.

16.6 To resolve a query about a Participant, such as from a Service Provider, the Interchange Directory MUST return a unique DID (decentralized identifier) for that Participant and MUST simultaneously disclose to the Participant that it has done so.

16.7 Unique Participant DIDs, one per service provider and issuer, MUST be generated when a Participant is listed in an Interchange Directory.

16.8 A Participant MAY request that they be delisted from an Interchange Directory in accordance with their local data privacy laws.

16.9 An Interchange Directory MUST comply with a valid delisting request in accordance with local and jurisdictional data retention policies.

16.10 A Interchange Directory MUST log all delisting requests in accordance with applicable data privacy regulation.

16.11 The ADI Association MUST periodically audit Interchange Directories for compliance with delisting requests, log retention policies, and security policies as per local regulation requirements. This MAY be done directly or or delegated to a third-party auditor.

17. Global Policies on Regions

17.1 As the ADI Association expands and the ADIA Specification extends to other regions, the ADI Association will, at the respective regional level, adapt the ADIA Specification Governance Framework, where necessary and under expert guidance, to incorporate region-specific policies, guidelines, and procedures for Issuers, Interchanges, and Interchange Service Providers.