DRAFT

Accountable Digital Identity Association (ADIA)

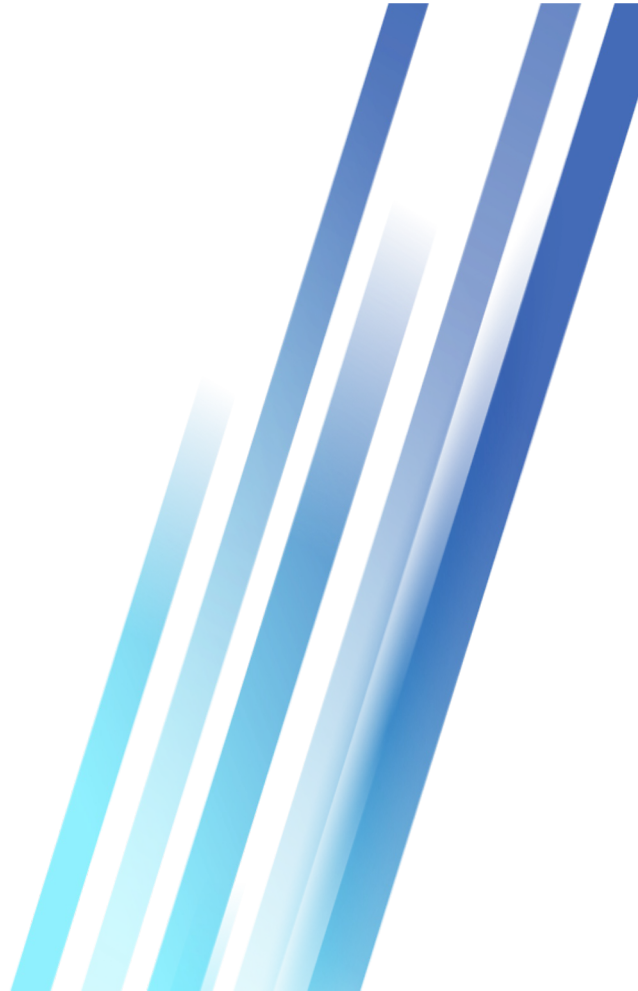
Technology Architecture

Jun-2022

Kiran Addepalli
Co-chair ADIA Technology Working Group/
VP of Engineering Digital Trust Networks

Agenda

1. ADIA Overview
2. ADIA Directories
3. What is a Digital Address
4. Data Model and Data Residency
5. Protocol Extensions
6. Compliance



DRAFT

Origin of ADI Association

ADI Association

2024-Future	**Business and Economic** Identity Marketplace Payment Models Certification and Education Cross-ledger settlements Contract Negotiation
2020-2023	**Identity and Control** On-board Users and Entities Identity Proofing Services Authentication and Consent Secure Storage/ Escrow Services Device Management and Recovery Audit and Compliance
2019 Existing Standards and Technology	**Data and Communication** Decentralized Identifiers (DID) Distributed Ledger (DLT) Verifiable Credentials (VC) DID Communication (DIDComm)

DRAFT

ADIA Members

ADI Association

CVS

RAON

IDEMIA

Early Warning

digital trust networks

badge

nok nok

HITACHI

30+ more founding members and growing…

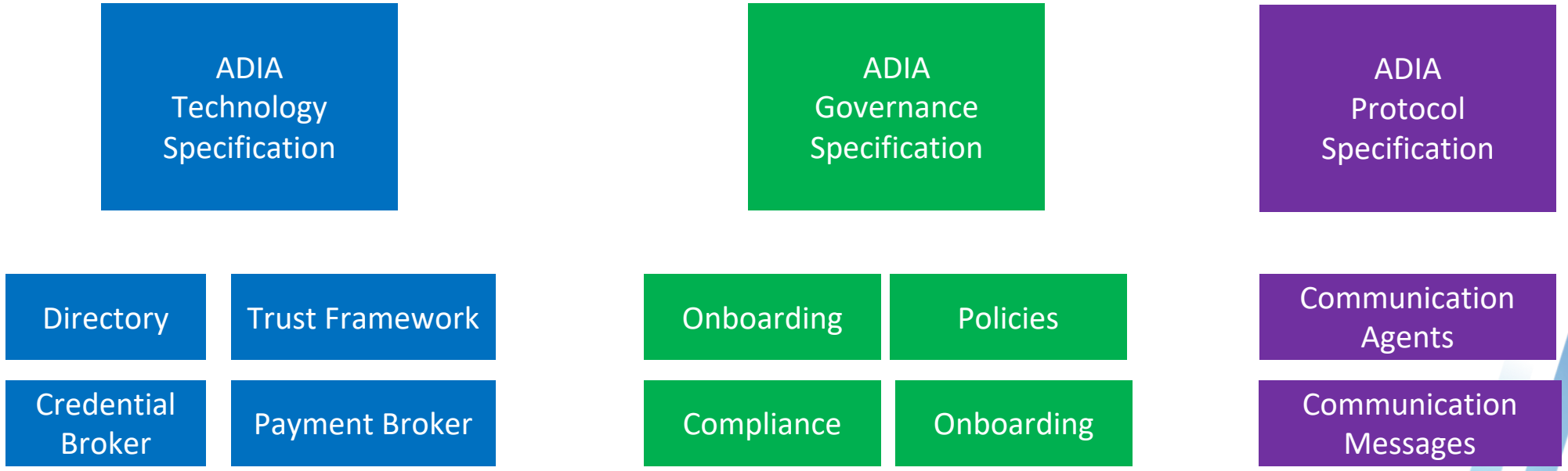
DRAFT

Opinionated Views

Trusted Onboarding of Parties	Starts with a Trusted Issuer Onboarding the User which provides a stronger Foundation/Framework for Trust and Accountability
Human Identity Binding	Each identity is cryptographically and biometrically bound to a specific human being. Users cannot pretend to be someone they are not. Even if a user has multiple DIDs, they will all point back to that specific user for accountability.
User Consent and Pre-consent	VCs can be presented by a cloud agent. Users can pre-consent to share certain data or delegate consent to trusted individuals. The cloud agent can present VCs even when the user's mobile wallet is unavailable.
Recoverability	VCs can be held by the issuer or in a cloud storage, with only VC copies or metadata held in the mobile wallet. Easy for users to migrate to or add another device. Adding a second device using a first device is effortless
Inclusivity	Supports Smart Cards as VCs can be presented from a cloud agent and only not from the mobile device.

DRAFT

ADIA Specification

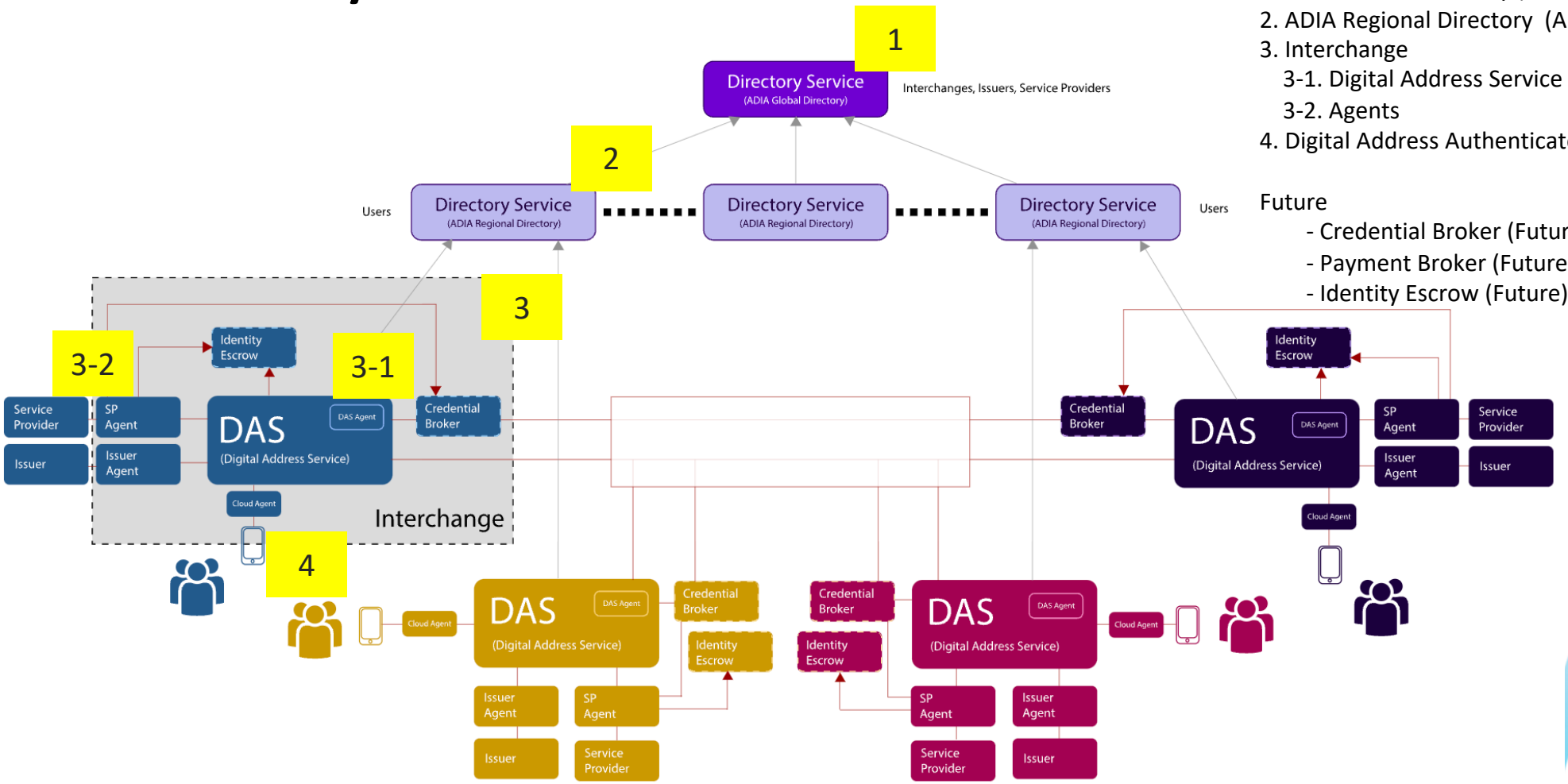


Status
Editor's Draft Version 1: November 2021
Version 2: Planning (Join Us! Collaboration is welcome!!)

Links to Technical and Governance Specifications are in the Appendix

DRAFT

ADIA Ecosystem



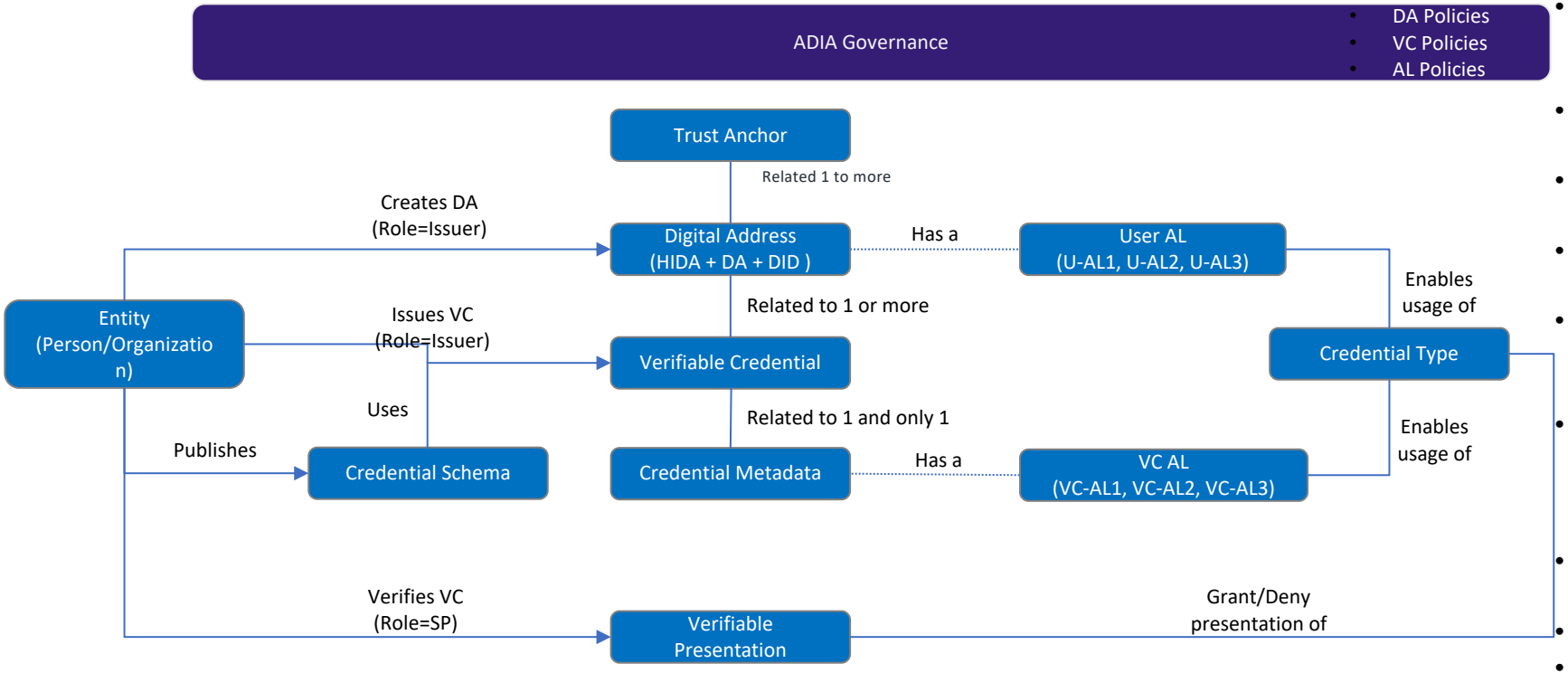
1. ADIA Global Directory (AGD)
2. ADIA Regional Directory (ARD)
3. Interchange
   3-1. Digital Address Service (DAS)
   3-2. Agents
4. Digital Address Authenticator (DAA)

Future
- Credential Broker (Future)
- Payment Broker (Future)
- Identity Escrow (Future)

ADIA Identifiers

Digital Address	Alias to a User or an Entity's DID issued by a trusted Digital Address Issuer. Looks like kiran.addepalli.us@dtx [US -> Country of Residence, DTX -> Identifier of the Interchange] May be modified by the User
HIDA	Cryptographic Hash of the ID-Attributes used to check uniqueness. Non-biometric information. Not persisted on the Ledger
HomeDAS	The Digital Address Service the User or Entity belongs to.
I-AL **VC-AL** **U-AL**	Assurance Level associated with the Issuer, Verifiable Credential issued by the Issuer and the User

Relationship between Core entities



- Digital Address has a one-to-one mapping with a Person/ User.
- Each DA/DID has a 1-to-1 relationship with a Trust Anchor. The Trust Anchor is not derived from any User attributes.
- The HIDA is generated by an Issuer Agent using the User identity attributes.
- The Primary DID remains constant throughout the lifecycle of the User
- Each User DID has a pairwise DID for connections with other entities to avoid correlation.
- The Digital Address may change but at any point in time, there is a 1-to-1 mapping with the corresponding DID
- The HIDA associated with the Digital Address may change depending on the level of information provided by the user at the time of creation of the Digital Address
- Each VC is related to one Credential Schema and Version.
- Each VC is related 1-to-1 with its Credential Metadata
- Depending on the HIDA attributes provided, the User Assurance Level is determined. This is defined as a policy at the ADIA Global Directory.

Roles

Issuers

Digital Address + Verifiable Credentials

- Create a Digital Address using attributes unique to the user
- Issues one or more Verifiable Credentials using information in HR or IAM systems
- Cryptographically signed by the Issuer of the Verifiable Credential

User

Identity Proofing

Prove the identity of the user acquiring the Digital Address

ID Proofing methods ex:

- Jumio
- IDEMIA
- EWS

Authentication and Device binding

- FIDO

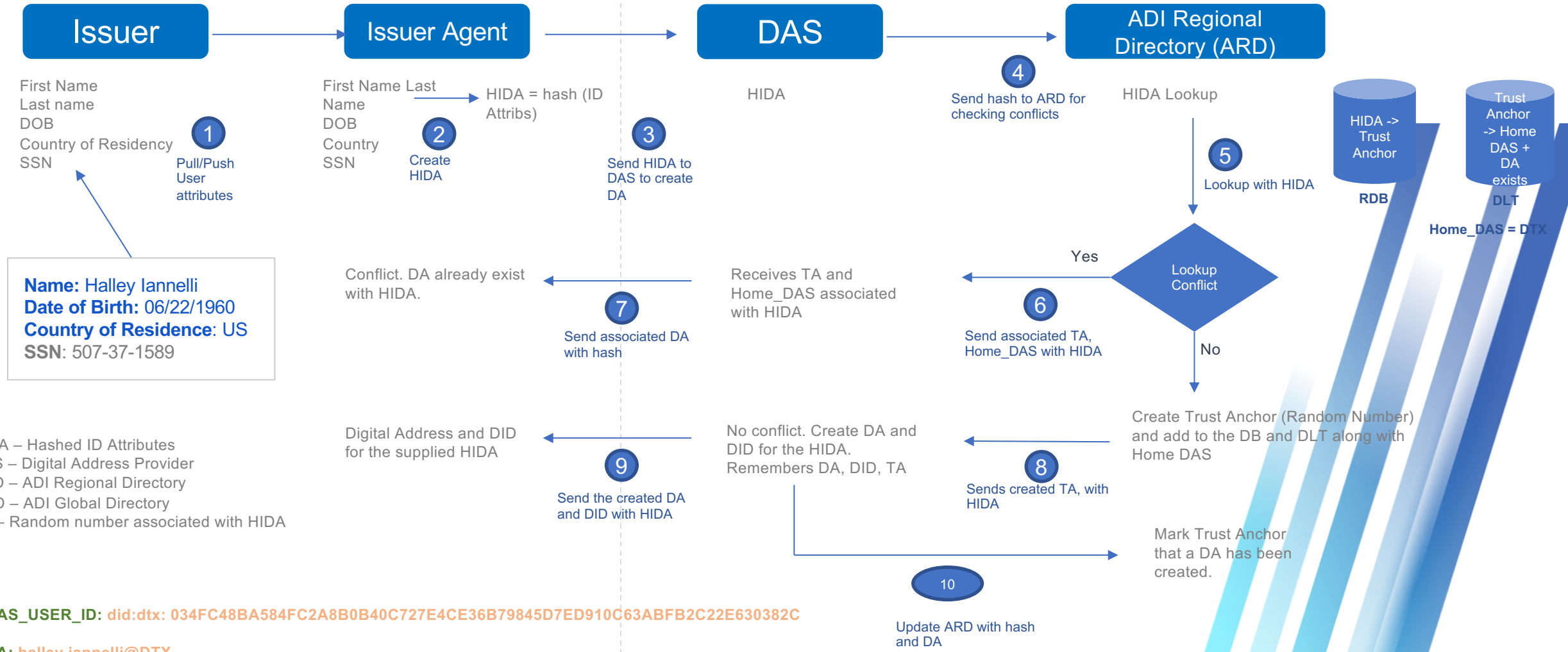
Service Providers

Verify Credentials

- Define rules to verify the user based on one or more claim attributes in the Verifiable Credentials
- Conforms to a Credential Schema
- Cryptographically verify information about the user and Issuer

DRAFT

How is a Digital Address Created



Name: Halley Iannelli
Date of Birth: 06/22/1960
Country of Residence: US
SSN: 507-37-1589

HIDA – Hashed ID Attributes
DAS – Digital Address Provider
ARD – ADI Regional Directory
AGD – ADI Global Directory
TA – Random number associated with HIDA

DAS_USER_ID: did:dtx: 034FC48BA584FC2A8B0B40C727E4CE36B79845D7ED910C63ABFB2C22E630382C

DA: halley.iannelli@DTX

Progressive HIDA (Same Person over time)

Timeline

T0 Only few HIDA Attributes available (FN,LN, Country of Residence)

T1 User Provides additional attributes – Ex: DoB

T2 User Provides additional attributes – Ex: SSN, National Identifier, Verification in Person, etc.

Trust Anchor (On-Ledger)

TA (Trust Anchor)	Entity ID	Home DAS ID (Digital Address Service)
bbcb15a0-c08f-42c1-8b5c-02e49efa1f22	did:dtx:A2MkmGBc3yisjThvt4i2USoQGJGf2kz7z3CFMeGkDWabx5BB	did:dtx:A456kmGBc3yisjThvt4i2USoQGJGf2kz7z3CFMeGkDWabx888

HIDA (Off-Ledger)

TA (Trust Anchor)	HIDA (Hashed ID Attributes)	Entity ID	Entity DA (Digital Address)	HIDA Attributes	Status	Assurance Level
bbcb15a0-c08f-42c1-8b5c-02e49efa1f22	b09403f0f6298614318eaf9f4f5702658c8e3d94d21ccd1d695fcf7840677445	did:dtx:A2MkmGBc3yisjThvt4i2USoQGJGf2kz7z3CFMeGkDWabx5BB	kenny.eastmond.us@dtx	FN,LN,Country	Inactive	AL1
bbcb15a0-c08f-42c1-8b5c-02e49efa1f22	c09403f0f6298614318eaf9f4f5702658c8e3d94d21ccd1d695fcf7840677555	did:dtx:A2MkmGBc3yisjThvt4i2USoQGJGf2kz7z3CFMeGkDWabx5BB	kenny.eastmond.us@dtx	FN,LN,DOB, Country	Inactive	AL2
bbcb15a0-c08f-42c1-8b5c-02e49efa1f22	d09403f0f6298614318eaf9f4f5702658c8e3d94d21ccd1d695fcf7840677666	did:dtx:A2MkmGBc3yisjThvt4i2USoQGJGf2kz7z3CFMeGkDWabx5BB	kenny.eastmond.us@dtx	FN,LN,DOB, Country, SSN	Active	AL3

TA – Entity DID relationship unchanged

HIDA updated
Only one HIDA active at any point in time

HIDA Audit

AL governed by ADIA Policy

Different Users with same HIDA

Timeline

T0 Kermit Oddboy is an existing User
[Kermit, Oddboy,10/10/1975,US]

T1 Kermit Oddboy (2) requests DA with Same HIDA Attributes
[Kermit, Oddboy,10/10/1975,US]

Trust Anchor (On-Ledger)

TA (Trust Anchor)	Entity ID	Home DAS ID (Digital Address Service)
aacb15a0-c08f-42c1-8b5c-02e49efa1f11	did:dtx:A1MkmGBc3yisjThvt4i2USoQGJGf2kz7z3CFMeGkDWabx5AA	did:dtx:A456kmGBc3yisThvt4i2USoQGJGf2kz7z3CFMeGkDWabx888
bbcb15a0-c08f-42c1-8b5c-02e49efa1f22	did:dtx:A2MkmGBc3yisjThvt4i2USoQGJGf2kz7z3CFMeGkDWabx5BB	did:dtx:A456kmGBc3yisThvt4i2USoQGJGf2kz7z3CFMeGkDWabx888

HIDA (Off-Ledger)

TA (Trust Anchor)	HIDA (Hashed ID Attributes)	Entity ID	Entity DA (Digital Address)	HIDA Attributes	Status	Assurance Level
aacb15a0-c08f-42c1-8b5c-02e49efa1f11	aa9403f0f6298614318eaf9f4f5702658c8e3d94d21ccd1d695fcf78406774aa	did:dtx:A1MkmGBc3yisjThvt4i2USoQGJGf2kz7z3CFMeGkDWabx5AA	kermit.oddboy.us@dtx	FN, LN, DOB, Country	Active	AL2
bbcb15a0-c08f-42c1-8b5c-02e49efa1f22	aa9403f0f6298614318eaf9f4f5702658c8e3d94d21ccd1d695fcf78406774aa	did:dtx:A2MkmGBc3yisjThvt4i2USoQGJGf2kz7z3CFMeGkDWabx5BB	kermit.oddboy.us_2@dtx	FN,LN,DOB, Country	Active	AL2

TA – Entity DID Unique

Same HIDA but related to a different TA + Entity ID

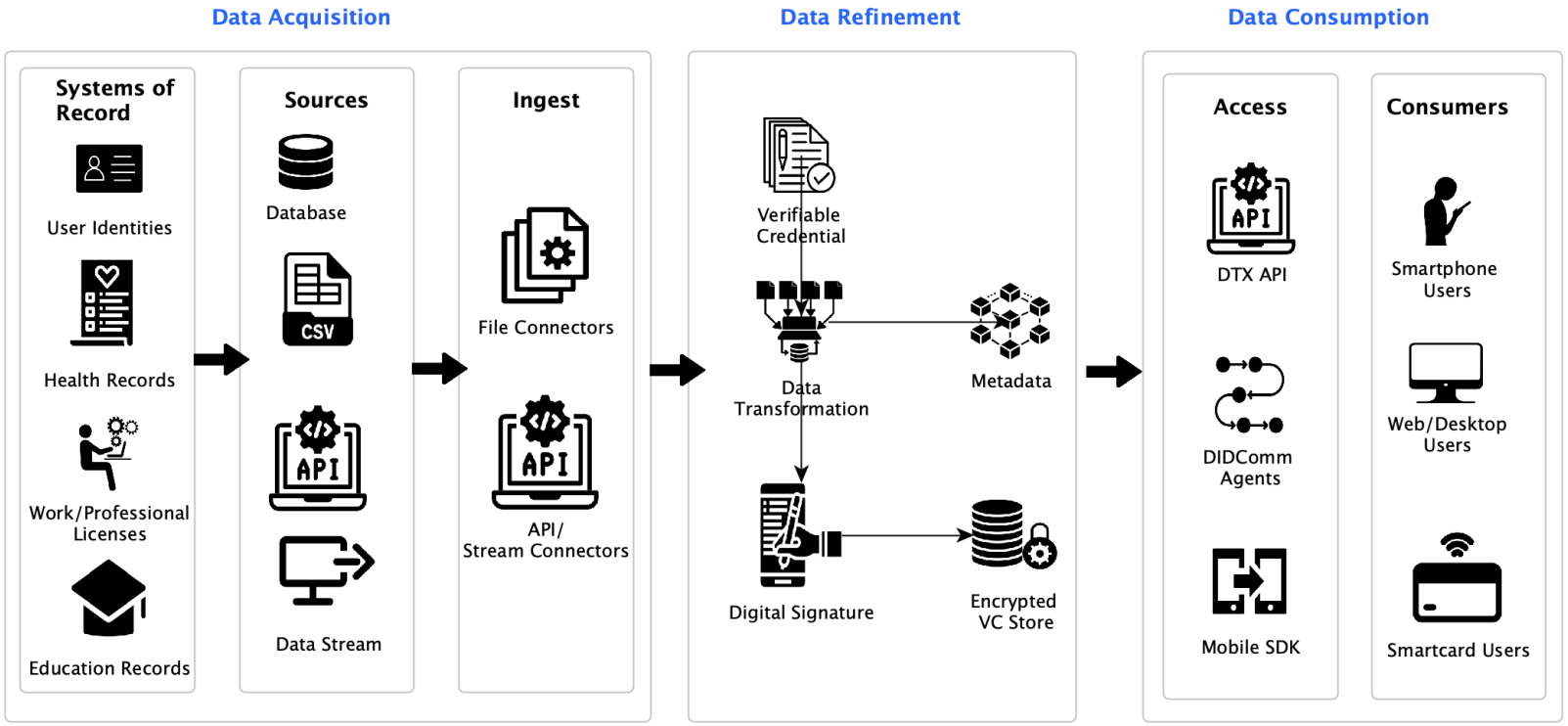
Cannot have the same DA

AL governed by ADIA Policy

ADI Association

Directories

Identity and VC Lifecycle



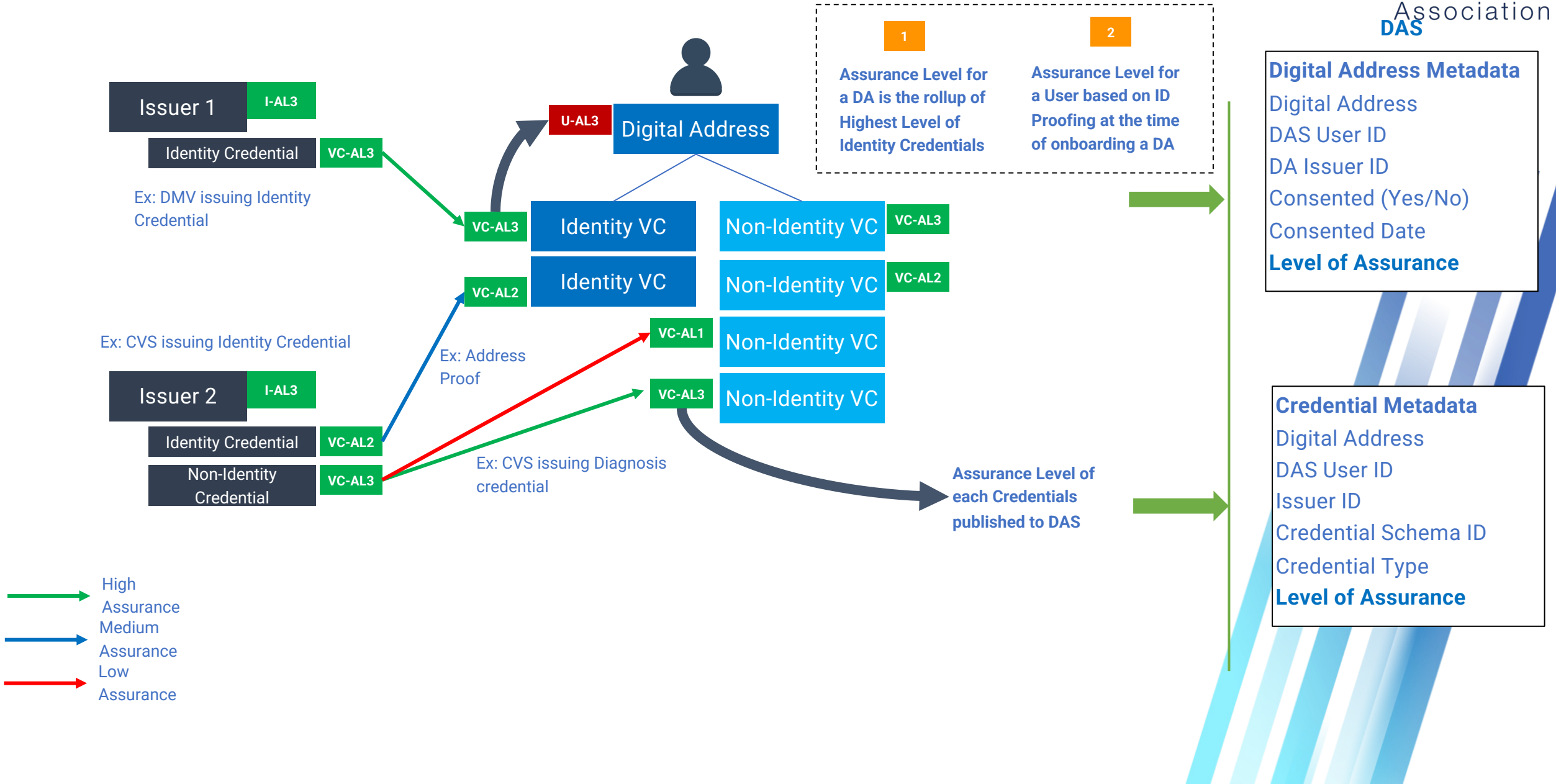
- Data resides at the source systems and does not cross system boundaries.
- Transform the raw datasets into Verifiable Credentials (VC) published by the ADIA Global Directory, ADIA Regional Directory, the Interchange or custom schema defined by the Tenant.
- Digitally sign the VCs using the Issuer's Keys and publish them to encrypted VC storage - either on-prem or in a service provided by the Interchange (Identity Escrow).
- Publish the VC metadata to the DAS DLT
- Provide access to the VC metadata using APIs
- Retrieve the VC information for presentation only by the Cloud Agent (DID Comm agents acting on behalf of the User or holder of the Verifiable Credential(s)).
- Consumers may get access to allowed VCs via web, mobile or a smart card after necessary authentication and verification of the private keys.

Where does data reside?

Issuer	DAS	User	ADIA Regional Directory	ADIA Global Directory
SaaS Model Tenant DB (Off-Ledger) • Encrypted VCs in VC Storage • Tenant Configuration • Tenant Policies • Custom VC Schema	**DLT** • Digital Address Metadata • VC Metadata • VC Schema published at the DAS and Issuer Level • User DIDDoc describing service endpoints	**Mobile Device** • VC Metadata • Digital Address and DID Information • FIDO Private Key	**DLT** • Trust Anchor for Users (TA, DID for User, Home DAS) • VC Schema published at the ARD Level	**DLT** • Map of DA-DID for ARDs, DAS, Service Providers and Issuers • DIDDocs for Issuers, Service Providers and Issuers • VC Schema published by the AGD
Hybrid Model (Optional) • Encrypted VCs in VC Storage • Issuer systems linking the Internal User with external Digital Address	**Off-Ledger** • FIDO Public Keys for all users • HIDA/ Digital Address Information • Audit Logs • Routing and Discovery Information	**SmartCard** • Digital Address and DID Information in Secure Element. • FIDO Private Key	**Off-Ledger** • HIDA/ Digital Address Information	**Off-Ledger** • Organization Details and Primary Contacts for ARDs, DAS, Service Providers and Issuers

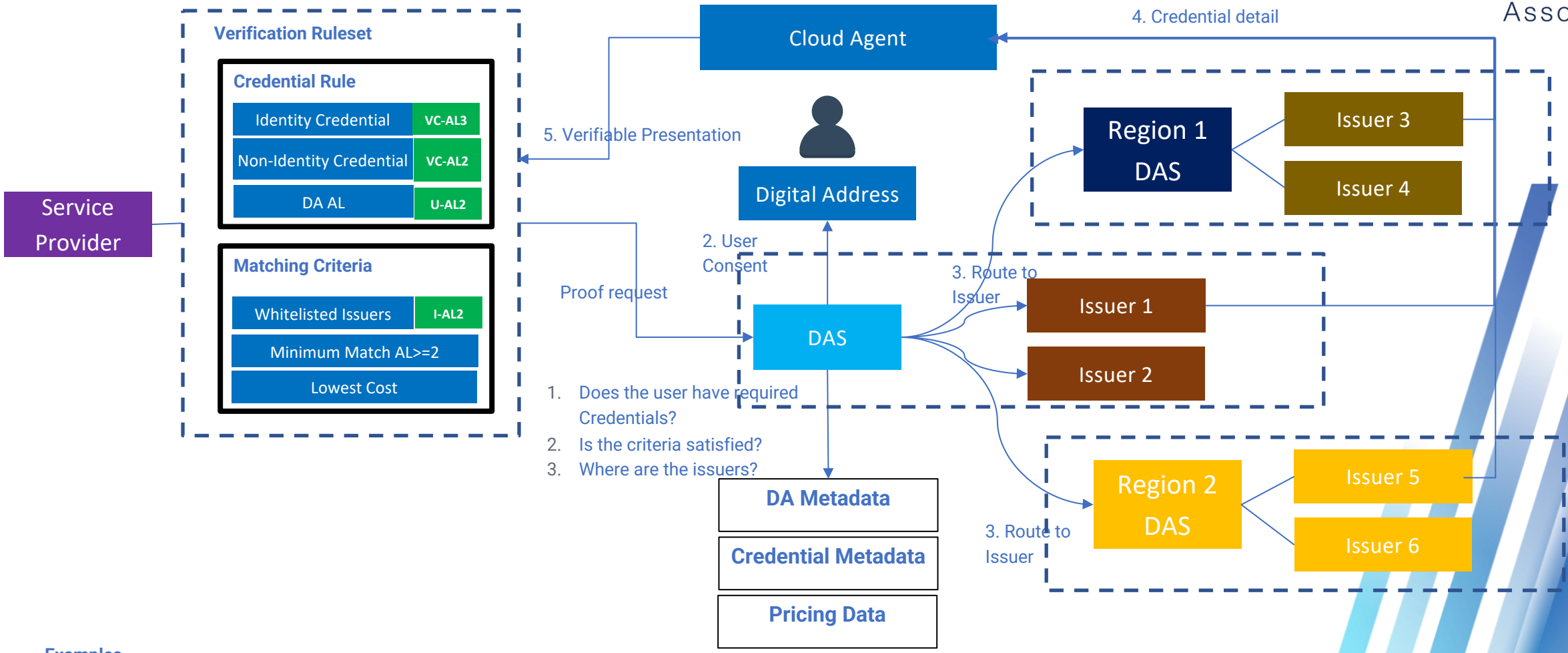
DRAFT

Issuance - VC + Assurance Level



DRAFT

Presentation - Credential Verification



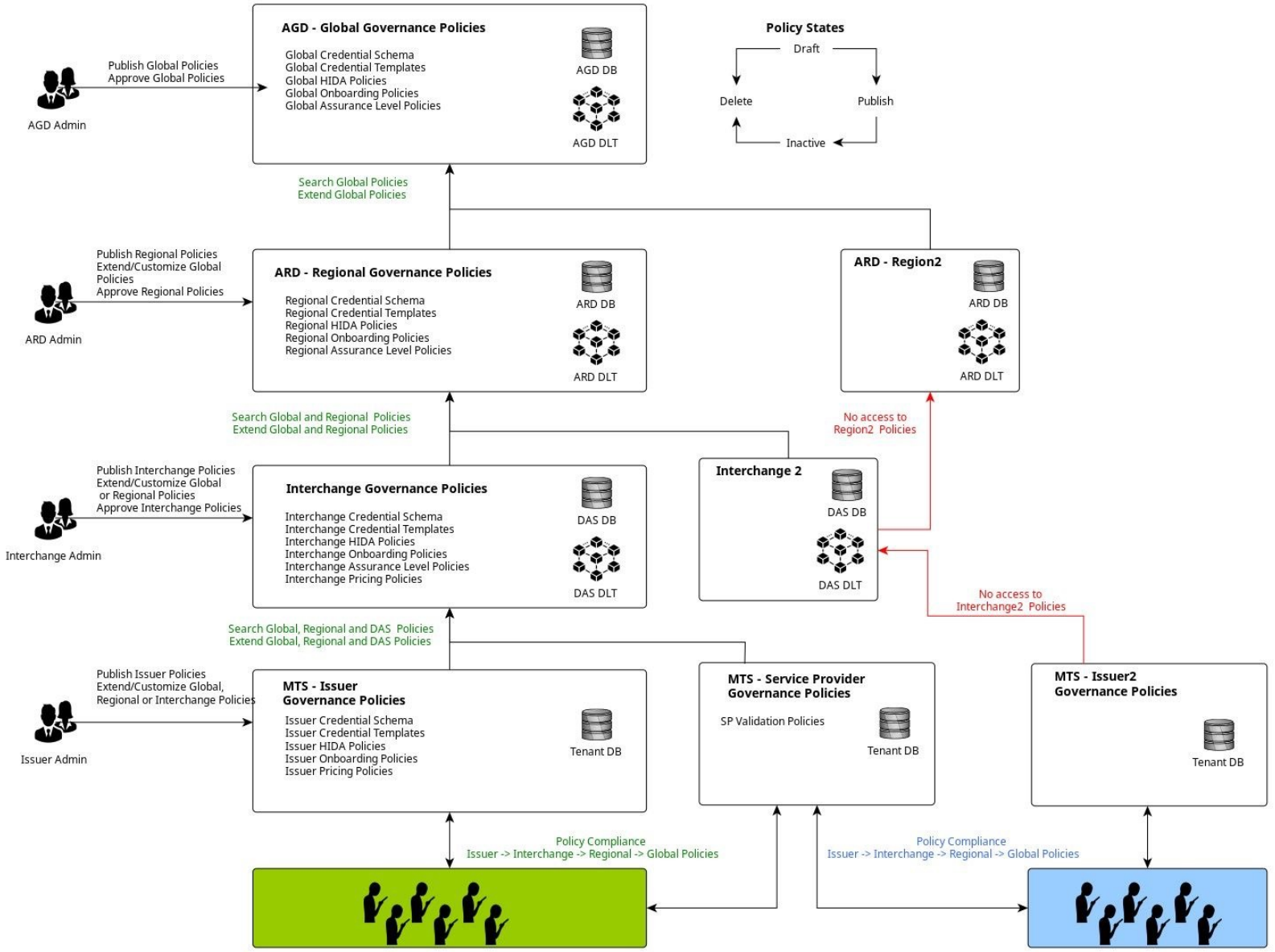
Examples

1. Employee onboarding service - Get the latest Identity information for a DA/DID with the least price.
2. Travel service - Get last N credentials (covid) with a negative result.
3. Mortgage service: Identity, Average income , Education, Credit Score credential

ADI Association

Compliance

What policies can you customize



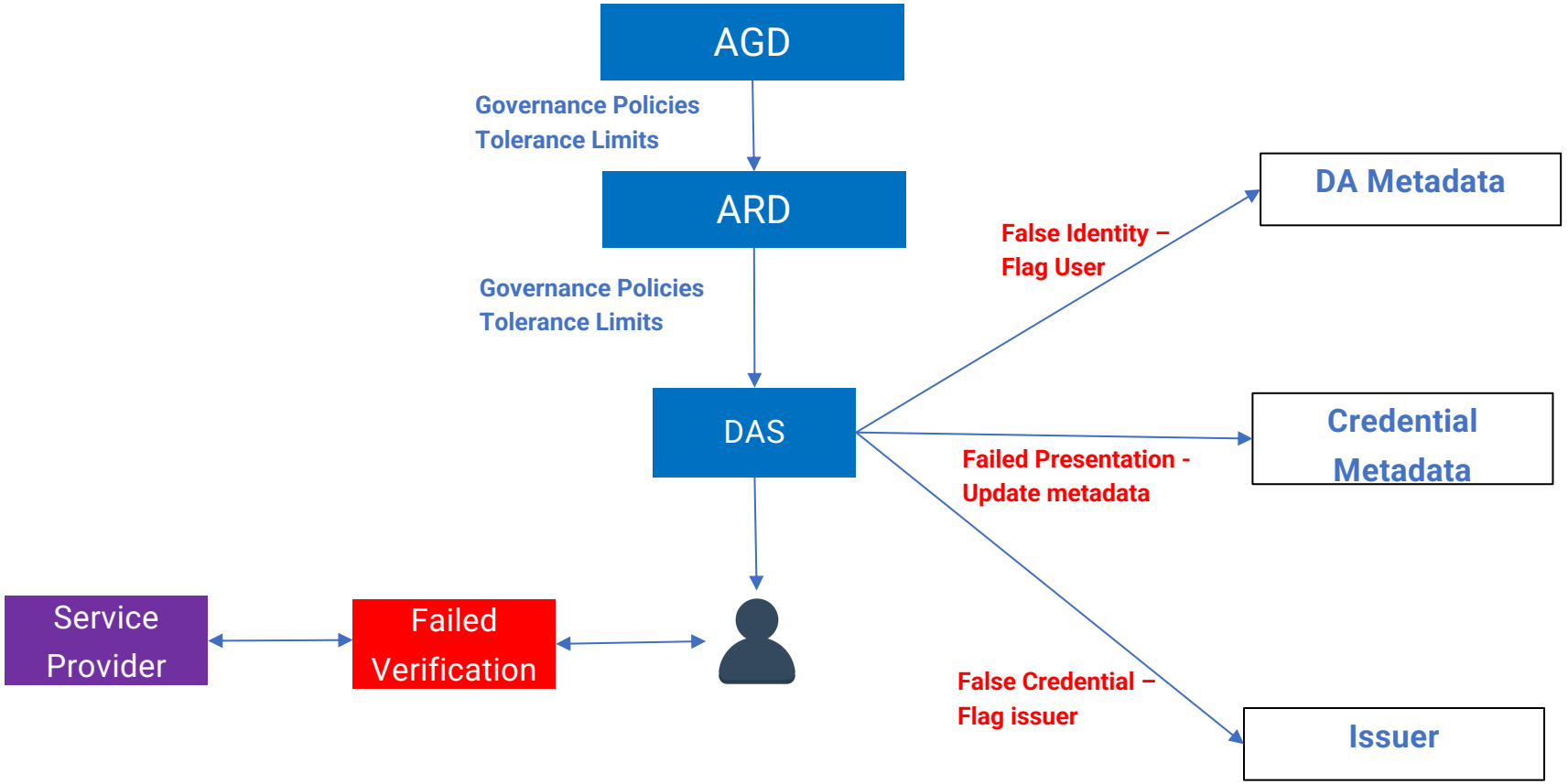
Policy Management and Compliance

- **Credential Schema** - Entities may define custom schemas or extend from the hierarchy chain.
- **Credential Templates** (Presentation Templates) - Customized presentation templates on a per issuer per schema basis.
- **HIDA policies** - Global and Regional policies that define the minimum number of attributes required and their Assurance Level mapping. This is further elaborated in the Progressive HIDA use cases.
- **Issuer Assurance Level Policies** - Policies that define the Issuer , types of credentials they are allowed to issue and their corresponding Assurance Levels.
- **Data Retention Policies** - Policies relating to audit data retention based on the compliance region.

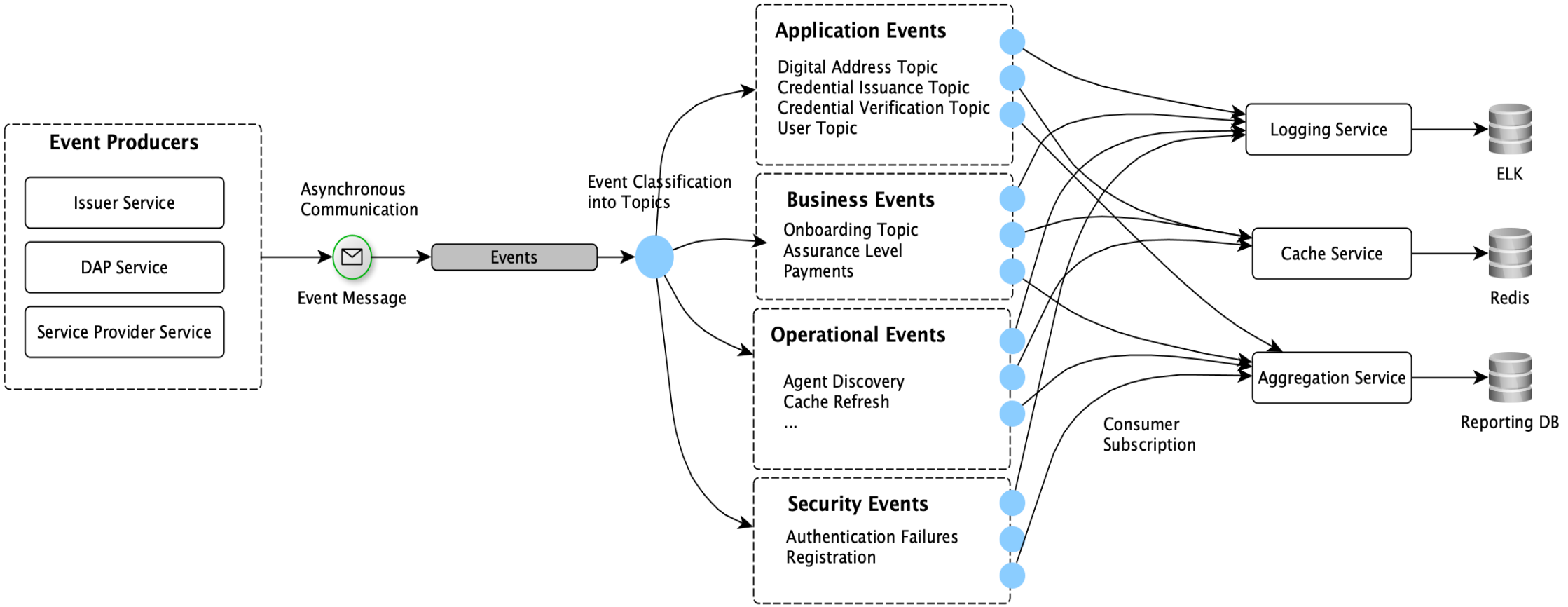
Additional policies relating to pricing, routing or discovery policies will be refined in subsequent releases

DRAFT

Detecting Bad Actors



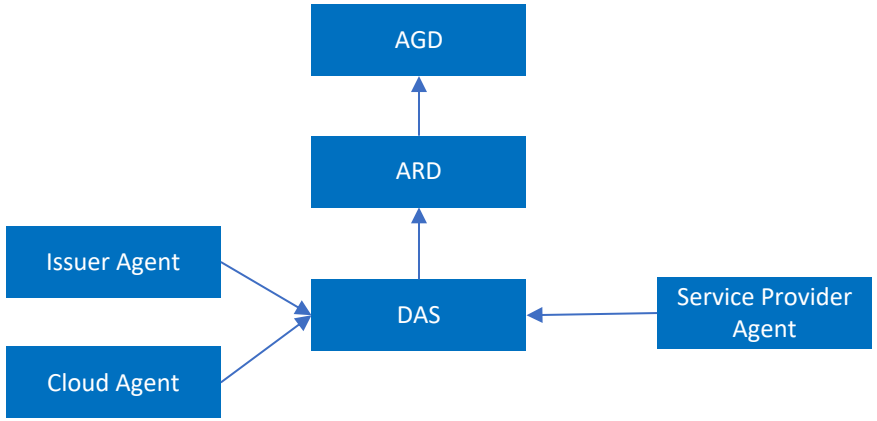
Auditing



ADI Association

ADIA Protocol

Communication

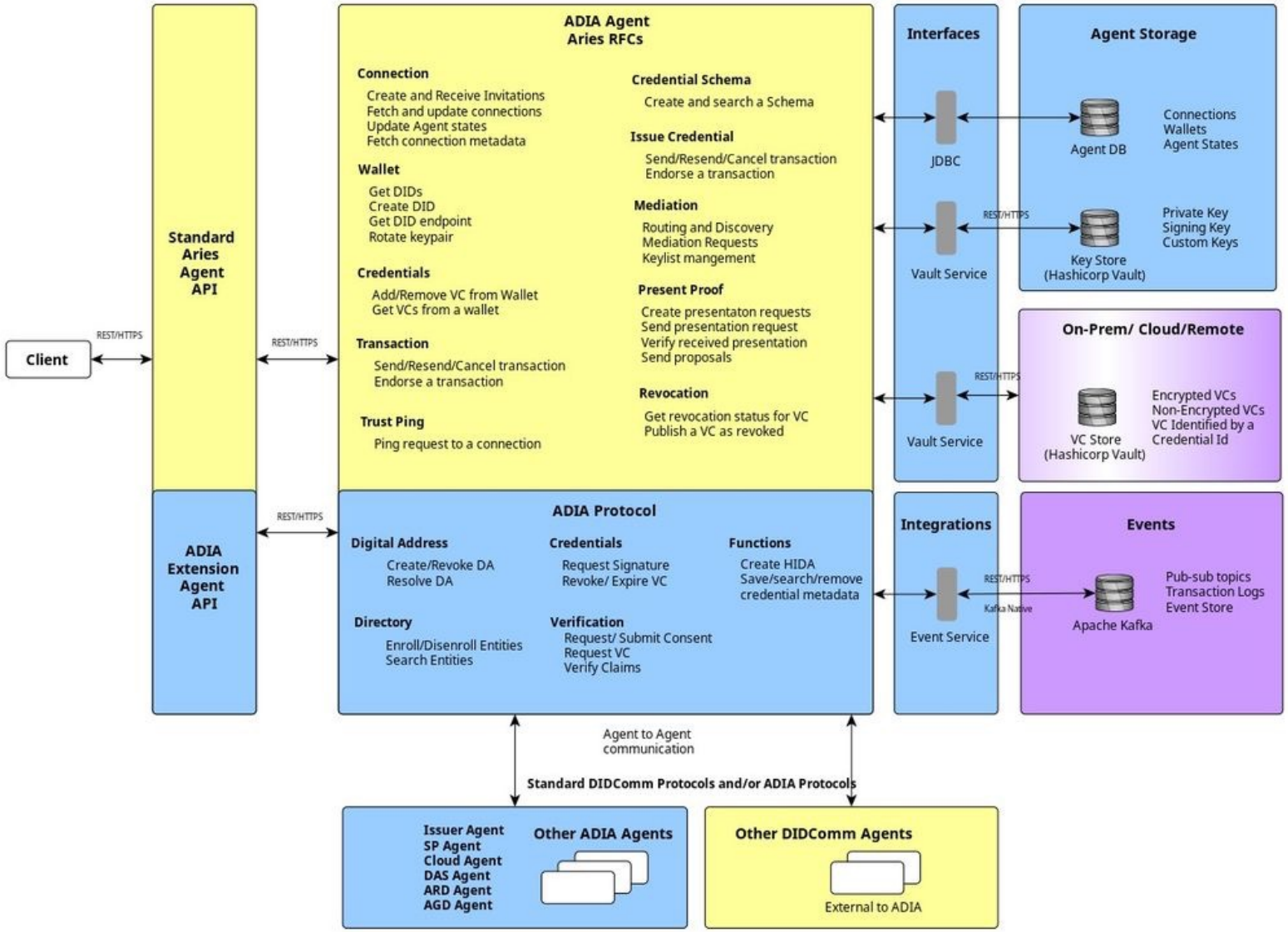


- Interactions are limited to certain entities by design
- Implementations may be using DIDComm or REST APIs

Agent-to-Agent communication matrix

Agent/Agent	AGD Agent	ARD Agent	DAS Agent	Issuer Agent	SP Agent	Cloud Agent
AGD Agent		X				
ARD Agent	X		X			
DAS Agent			X	X	X	X
Issuer Agent			X			X
SP Agent			X			X
Cloud Agent			X	X		X

DIDComm Agent extensions



DTX Implementation of the ADIA Agent has few other customizations:

- Persistent Agent Storage with connection and agent states in PostgreSQL
- Key Storage stored in Hashicorp Vault
- Separate VC storage in HashiCorp Vault either on Issuer's on-prem or managed by DTX in the Cloud
- Integrations with Kafka and other event stores.
- ADIA Agents can communicate with other ADIA agents or a standard DIDComm to exchange VCs across DASs

Verifiable Credentials

Process

- Issue a VC - https://adiassociation.github.io/ADIA-specification/ADIA-overview.html#sctn-issue-vc
- Revoke a VC - https://adiassociation.github.io/ADIA-specification/ADIA-overview.html#sctn-revoking-credential
- VC Presentation - https://adiassociation.github.io/ADIA-specification/ADIA-overview.html#sctn-iden-creds

VC Issuance

- VC payload signing, agents use **Ed25519 signature algorithm.** This is the only supported algorithm in the current implementation. In future releases, we can make it configurable
- The current implemented VC formats are derived from Indy implementation. However, only predicates are supported and evaluated at agent level with full disclosure of the VC attributes.
- Selective disclosure capability of the ZKP is planned with the use of JSON/JWT & BBS+ signature supported VCs

ADI Association

Next Steps

Advancement areas

- Ability to present VCs offline when no network is available
- Split core identity to be on device and non-identity credentials in the Cloud wallet
- Credential Schema and Content development in different regions.
- Zero-knowledge proofs

ADI Association

Appendix

References

Technical Specs

ADIA Technical Specification: https://adiassociation.github.io/ADIA-specification/ADIA-overview.html
ADIA Protocol: https://adiassociation.github.io/ADIA-specification/ADIA-protocol.html

Governance Specification

ADIA Specification Governance: https://adiassociation.github.io/ADIA-specification/ADIA-spec-governance.html
ADIA Corporate Governance: https://adiassociation.github.io/ADIA-specification/ADIA-corporate-governance.html

DRAFT

Digital Address Metadata

Name	Display Name	Type	Description
HIDA	Not Displayed	Text	Computed HASH of ID-attributes
name	Name	Text	Name of the Credential if replaced by the User
entityId	Not Displayed	Text	DID of the subject
entityDigitalAddress	Issued To	Text	DA of the subject
issuerId	Not Displayed	Text	DID of the Issuer of VC
issuerDigitalAddress	Issued By	Text	DA of the Issuer of VC
issuedDate	Issued On	DateTime	Time the VC was issued (Not the record)
consent_ind	Consent Indicator	Boolean	Indicator whether the entitiy has consented to creating the DA
consentedDate	Consented Date	DateTime	Date of consent
consentedBy	Consented By	Text	Consenting entity DID
active	Active?	Boolean	Status
assuranceLevel	Assurance Level	Enum	Assurance Level as defined by the Governance process

Name	Display Name	Type	Description
createdBy	Created By	Text	The DID of the user creating the Audit item
createdDate	Created On	DateTime	Created date. Mostly the issued date but not necessarily
revoked	Revoked?	Boolean	Is the status revoked?
revokedDate	Revocated On	DateTime	Time the VC was revoked
revokingEntityId	Not Displayed	Text	DID of the entity that revoked the credential. Mostly the Issuer but may not be necessarily in the future.
revokingEntityDigitalAddress	Revoked By	Text	DA of the revoking entity
dasId	Not Displayed	Text	HomeDAS Id
dasDigitalAddress	Not Displayed	Text	Home DAS DA
attributeNames	Displayed as list of values	Array[NameValue]	List of Attribute values

DRAFT

Credential Metadata

Name	Display Name	Type	Description
credentialId	Not Displayed	Text	Id of the credential in the VC Store
name	Name	Text	Name of the Credential if replaced by the User
credentialType	Type	Text	Type of the Credential
credentialSchemaId	Not Displayed	Text	Identifier of the Credential Schema against which the VC was issued
credentialSchemaVersion	Not Displayed	Text	Version of the Schema
credentialSchemaName	Not Displayed	Text	Name of the Schema
credentialDefinitionId	Not Displayed	Text	
entityId	Not Displayed	Text	DID of the subject
entityDigitalAddress	Issued To	Text	DA of the subject
issuerId	Not Displayed	Text	DID of the Issuer of VC
issuerDigitalAddress	Issued By	Text	DA of the Issuer of VC
issuedDate	Issued On	DateTime	Time the VC was issued (Not the record)
active	Active?	Boolean	Status
assuranceLevel	Assurance Level	Enum	Assurance Level as defined by the Governance process

Name	Display Name	Type	Description
createdBy	Created By	Text	The DID of the user creating the Audit item
createdDate	Created On	DateTime	Created date. Mostly the issued date but not necessarily
revoked	Revoked?	Boolean	Is the status revoked?
revokedDate	Revocated On	DateTime	Time the VC was revoked
revokingEntityId	Not Displayed	Text	DID of the entity that revoked the credential. Mostly the Issuer but may not be necessarily in the future.
revokingEntityDigitalAddress	Revoked By	Text	DA of the revoking entity
dasId	Not Displayed	Text	HomeDAS Id
dasDigitalAddress	Not Displayed	Text	Home DAS DA
attributeNames	Displayed as list of values	Array[NameValue]	List of Attribute values

Credential Schema (DTX Implementations)

Credential Schema	Credential Type	Schema Level	Description
HIDA Schema	Identity	AGD	A schema with Identity attributes specific to an individual. Identity VC is issued at the time of creating a Digital Address for the User
DriversLicense Schema	Identity	DAS	Needs to be aligned to the ISO/IEC FDIS 18013-5 at a later date. Currently US only
Passport Schema	Identity	DAS	Needs to align to Electronic Passports.
Patient Identity Schema	Identity, Health	DAS	Loosely aligned with HL7
Medical Insurance Schema	Identity, Health	DAS	Loosely aligned with HL7
Medication Schema	Health	DAS	Loosely aligned with HL7
Medical Condition Schema	Health	DAS	Loosely aligned with HL7
Immunization Schema	Health	DAS	Loosely aligned with HL7
Allergy Schema	Health	DAS	Loosely aligned with HL7
Healthcare Worker Schema	Experience, Health	DAS	Loosely aligned with HL7
Diagnosis Record Schema	Health	Issuer	Aligned with CCI Credentials. Recommended to move to HL7 standards for Lab Tests and Lab Results
Education Schema	Education	DAS	No current standards to align
Experience Schema	Experience	DAS	No current standards to align
Professional License Schema	Experience	DAS	No current standards to align