

# 2022-06-13 TSWG Meeting Notes

## Meeting Date

- 13 Jun 2022

## Zoom Meeting Link / Recording

- [https://zoom.us/rec/share/ghCvC\\_bWm8eFxlUPnkEXbMEwTNJ-vgzR5ngSUF6waKea0NFwr2M\\_gH\\_cUrbdpstU.Qek-8JzbCFBuJmoq](https://zoom.us/rec/share/ghCvC_bWm8eFxlUPnkEXbMEwTNJ-vgzR5ngSUF6waKea0NFwr2M_gH_cUrbdpstU.Qek-8JzbCFBuJmoq)

## Attendees


- [Darrell O'Donnell](#)
- [Drummond Reed](#)
- [sankarshan](#)
- [Judith Fleenor](#)
- Kiran Addepalli, ADIA
- Abbie Barbir, ADIA
- (another ~12 attendees whose names were not recorded)

## Main Goals of this Meeting

A special presentation about [The ADI Association](#) from Kiran Addepalli, Co-Chair of the ADIA Technical Working Group and VP of engineering of Digital Trust Networks.

## Agenda Items and Notes (including all relevant links)

Time	Agenda Item	Lead	Notes
3 min	<ul style="list-style-type: none"><li>• Start recording</li><li>• Welcome &amp; antitrust notice</li><li>• Introduction of new members</li><li>• Agenda review</li></ul>	Chairs	<ul style="list-style-type: none"><li>• <b>Antitrust Policy Notice:</b> <i>Attendees are reminded to adhere to the meeting agenda and not participate in activities prohibited under antitrust and competition laws. Only members of ToIP who have signed the necessary agreements are permitted to participate in this activity beyond an observer role.</i></li><li>• New Members:</li></ul>
2 mins	Review of Action Items from the previous meeting	Chairs	<ul style="list-style-type: none"><li>✓ ACTION: Wenjing Chu and Vikas Malhotra to draft a wiki page for the charter of an AI Identity Trust Issue Task Force.<ul style="list-style-type: none"><li>◦ The charter has been published: <a href="#">AI &amp; Metaverse Technology Task Force (DRAFT)</a></li><li>◦ ACTION: Members of TSWG to review <a href="#">the draft charter for the AI &amp; Metaverse Technology Task Force</a> for discussion and action at the next meeting.</li><li>◦ ACTION: <a href="#">Drummond Reed</a> to schedule this review for the next meeting.</li></ul></li></ul>
5 mins	Task Force Reports	TF Leads	We skipped TF reports in this meeting to provide more time for the ADIA presentation.

4 5 m ins	Special presentation about <a href="#">The ADI Association</a>	Kiran Addepalli	<p>Kiran's full presentation is attached here. See also screenshots #1 thru #14 below.</p> <div data-bbox="420 161 922 661">  <p>ADIA Tech Architecture - ToIP.pdf</p> </div> <p>The topics Kiran covered included 1-4 of the list below</p> <ol style="list-style-type: none"> <li>1. ADIA Directory Services</li> <li>2. Digital Address and how do you get one</li> <li>3. Relationship between core entities</li> <li>4. Credential Metadata – What is stored and where</li> <li>5. DIDComm extensions</li> <li>6. Policies and customizations</li> </ol> <p>Darrell asked about next steps. The next meeting with the ADIA team is this coming Thursday, 16 June, at 11:00-12:00 PT / 18:00-19:00 UTC. It will focus on the business and governance structure of ADIA.</p> <p>A subsequent meeting on the ADIA protocol stack and how it fits with the ToIP stack will be scheduled as soon as it is convenient.</p>
5 m ins	<ul style="list-style-type: none"> <li>• Review decisions /action items</li> <li>• Planning for next meeting</li> </ul>	Chairs	

## Screenshots/Diagrams (numbered for reference in notes above)

#1

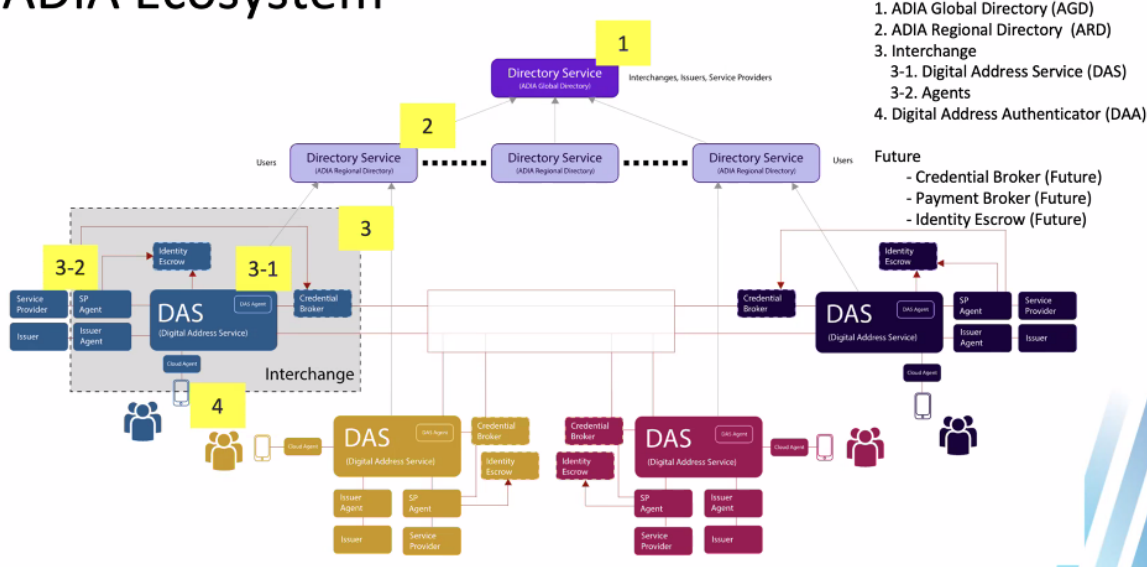
# Origin of ADI Association



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)	

#2

## ADIA Ecosystem



#3

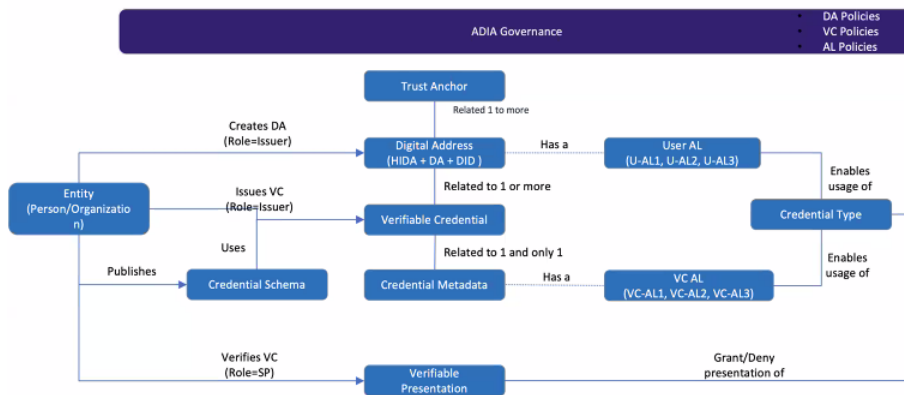
## ADIA Identifiers



Digital Address	Alias to a User or an Entity's DID issued by a trusted Digital Address Issuer. Looks like <a href="#">kiran.adddepalli.us@dtx</a> [ 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

#4

# 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.

#5

## 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

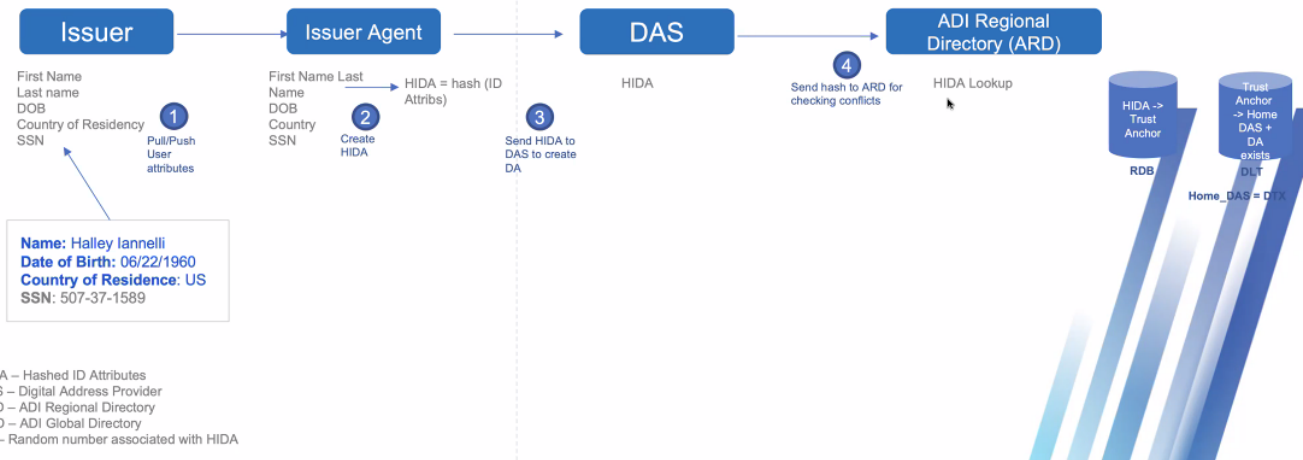
### Service Providers

#### 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

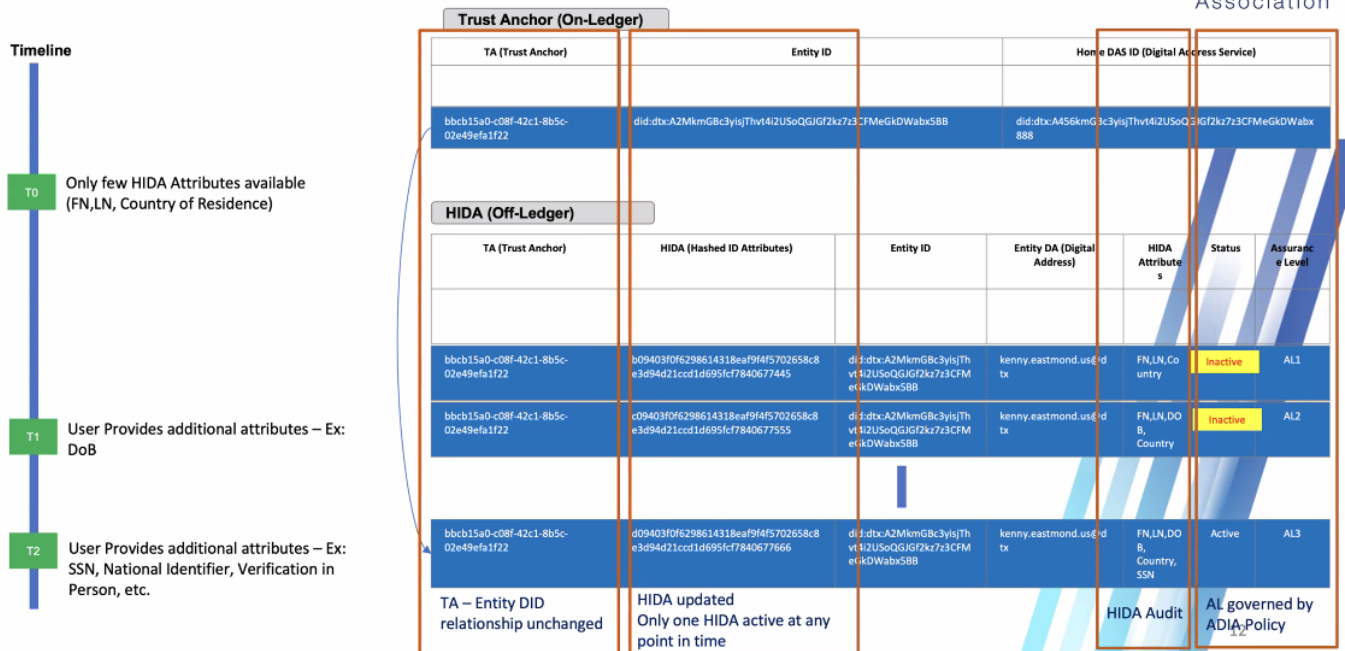
#6

# How is a Digital Address Created



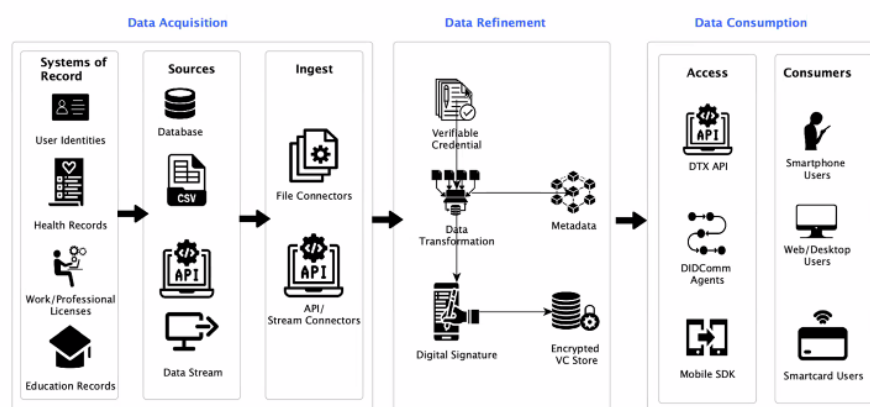
#7

# Progressive HIDA (Same Person over time)



#8

# 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.

#9

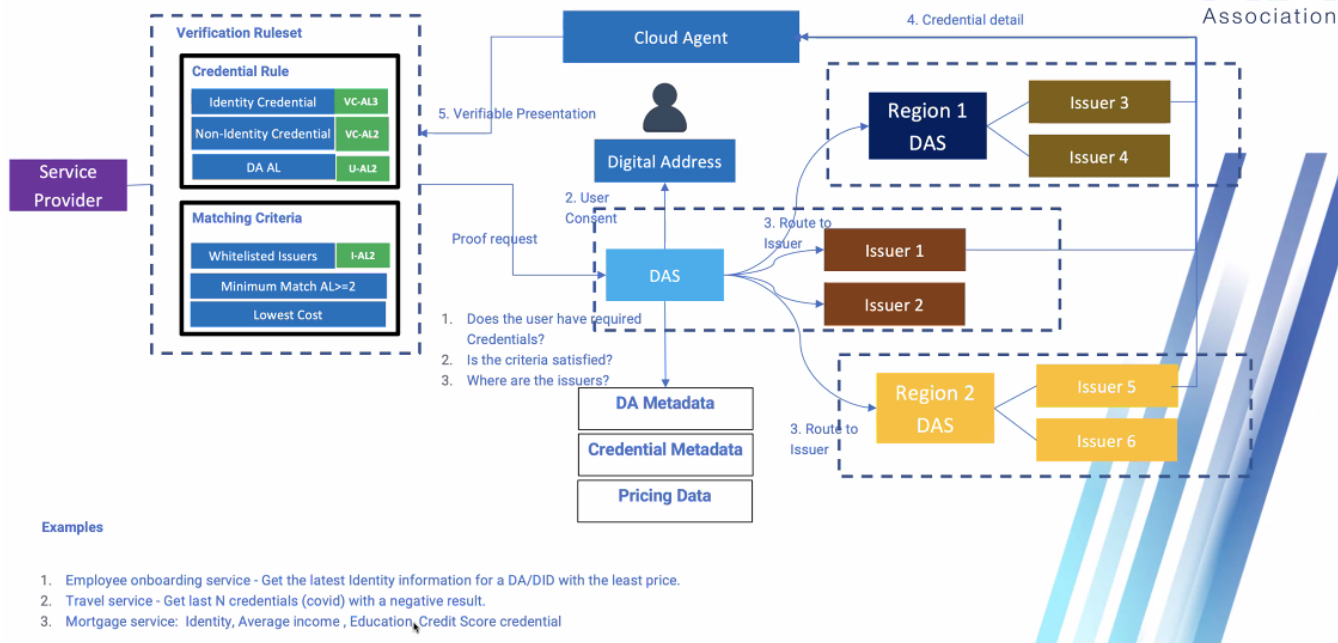
## Where does data reside?

Issuer	DAS	User	ADIA Regional Directory	ADIA Global Directory
<b>SaaS Model</b> Tenant DB (Off-Ledger) <ul style="list-style-type: none"> <li>• Encrypted VCs in VC Storage</li> <li>• Tenant Configuration</li> <li>• Tenant Policies</li> <li>• Custom VC Schema</li> </ul>	<b>DLT</b> <ul style="list-style-type: none"> <li>• Digital Address Metadata</li> <li>• VC Metadata</li> <li>• VC Schema published at the DAS and Issuer Level</li> <li>• User DIDDoc describing service endpoints</li> </ul>	<b>Mobile Device</b> <ul style="list-style-type: none"> <li>• VC Metadata</li> <li>• Digital Address and DID Information</li> <li>• FIDO Private Key</li> </ul>	<b>DLT</b> <ul style="list-style-type: none"> <li>• Trust Anchor for Users (TA, DID for User, Home DAS)</li> <li>• VC Schema published at the ARD Level</li> </ul>	<b>DLT</b> <ul style="list-style-type: none"> <li>• Map of DA-DID for ARDs, DAS, Service Providers and Issuers</li> <li>• DIDDocs for Issuers, Service Providers and Issuers</li> <li>• VC Schema published by the AGD</li> </ul>
<b>Hybrid Model (Optional)</b> <ul style="list-style-type: none"> <li>• Encrypted VCs in VC Storage</li> <li>• Issuer systems linking the Internal User with external Digital Address</li> </ul>	<b>Off-Ledger</b> <ul style="list-style-type: none"> <li>• FIDO Public Keys for all users</li> <li>• HIDA/ Digital Address Information</li> <li>• Audit Logs</li> <li>• Routing and Discovery Information</li> </ul>	<b>SmartCard</b> <ul style="list-style-type: none"> <li>• Digital Address and DID Information in Secure Element.</li> <li>• FIDO Private Key</li> </ul>	<b>Off-Ledger</b> <ul style="list-style-type: none"> <li>• HIDA/ Digital Address Information</li> </ul>	<b>Off-Ledger</b> <ul style="list-style-type: none"> <li>• Organization Details and Primary Contacts for ARDs, DAS, Service Providers and Issuers</li> </ul>

#10

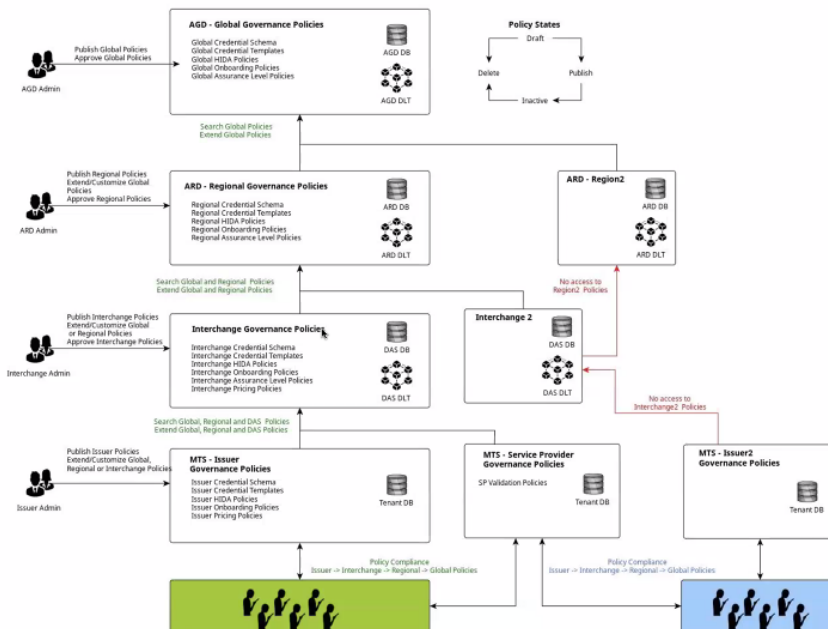


# Presentation - Credential Verification



#11

# What policies can you customize



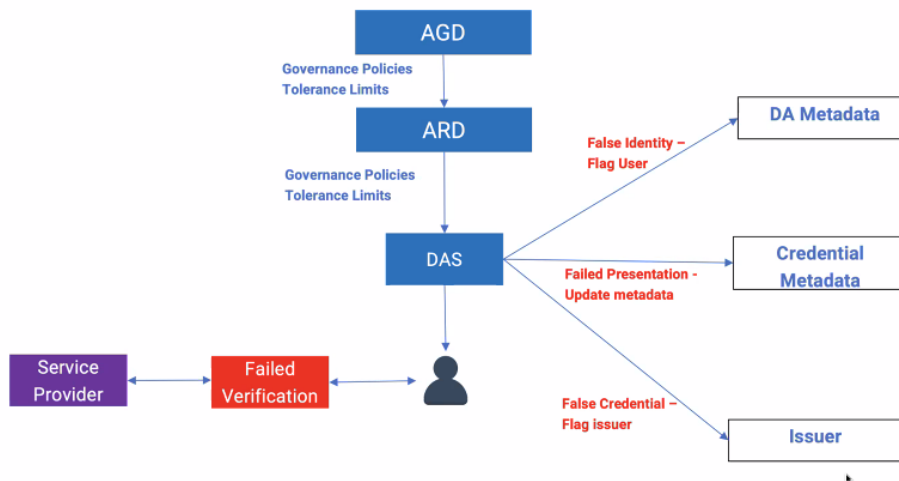
## Policy Management and Compliance

- 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

#12

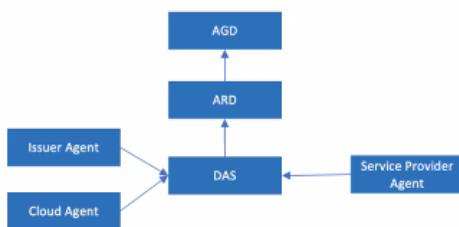
# Detecting Bad Actors



#13

## Communication

Agent-to-Agent communication matrix



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

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

#14

## 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



## Decisions

☐ None

## Action Items

- ☐ ACTION: Members of TSWG to review [the draft charter for the AI & Metaverse Technology Task Force](#) for discussion and action at the next meeting.
- ☐ ACTION: [Drummond Reed](#) to schedule this review for the next meeting.