OPEN IDENTITY EXCHANGE

Making Digital ID a Success

Global Trust Frameworks Interoperability

Nick Mothershaw
Chief Identity Strategist

OIX Global Interoperability Working Group

In support of the GAIN Initiative.

Objective:

- **Determine what is needed to allow IDs from one trust framework to accepted in another trust framework.**

Working Group members include:

Barclays, Deloitte, Lexis Nexis, Microsoft, NatWest, Sopra Steria, Assurant Consulting, Condatis, Credas, Considrd Consulting, Credas, Digidentiy, Digtal Identity Net, GBG, GLEIF, Hooyu, IAG, ID Crowd, IIF, InfoNetworks, mVine, Nuggets, Onfido, OIDF, TISA, tScheme, YOTI and the UK Government.

DGX paper – February 2022

Highlights that endorse our objectives

Covers ID and Eligibility Information

However, the working group recognised that both mutual recognition and interoperability are complex challenges that will take several years to achieve. They require policy, legal and technical alignment between government trust frameworks, digital identities, and infrastructure. Efforts to enable interoperability, such as the EU's eIDAS, show these challenges are significant to overcome.

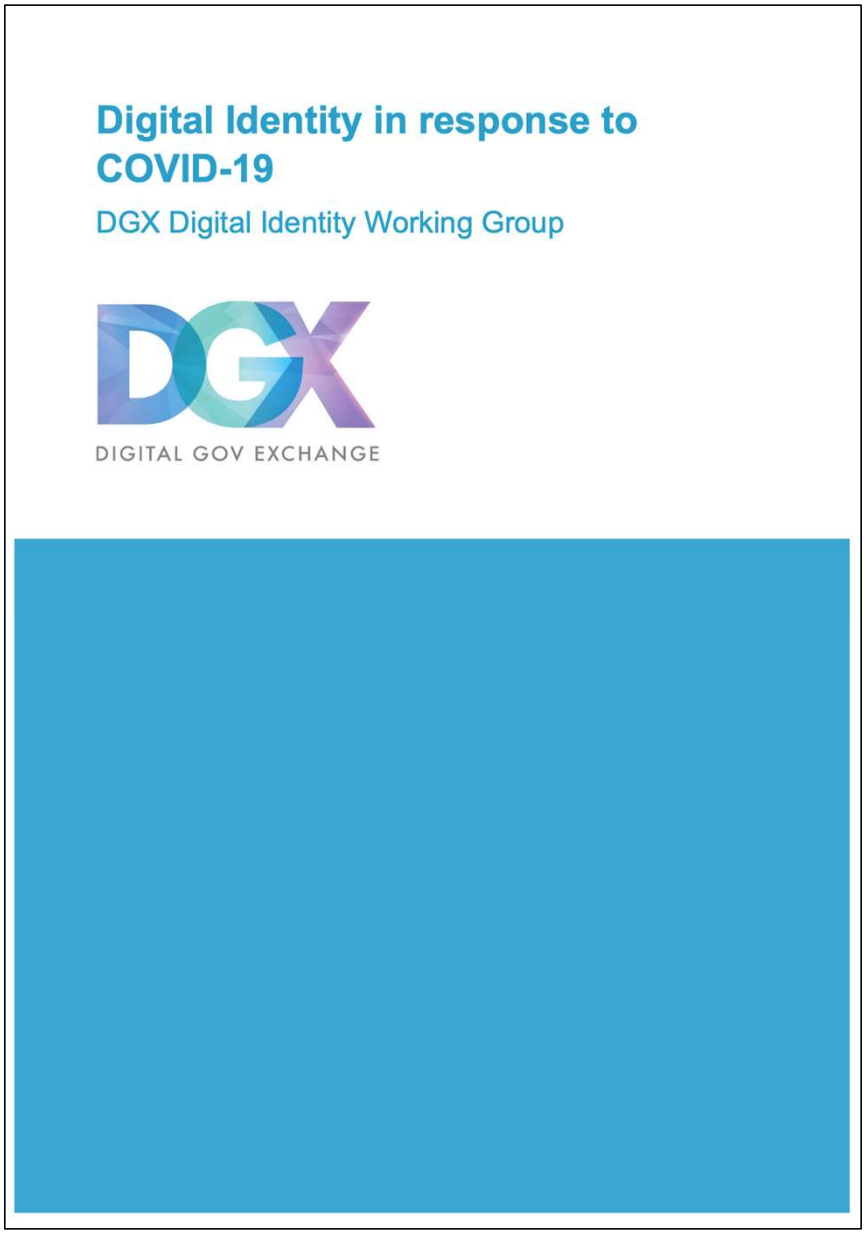
The DIWG identified foundational activities required to enable both mutual recognition and interoperability of digital identities, including:

- The definition of a common language and definitions across digital identities,
- Assessment and alignment of respective legal and policy frameworks, supported by appropriate consensus on identity standards and cross-border application, and
- Interoperable technical models and infrastructure.

However, differences in legislation and specific government requirements may also impact mutual recognition and interoperability. This includes issues such as differing views on or misalignment between privacy and personal data legislation, security and data sovereignty across borders, and the role of government and the private sector in digital identity systems.

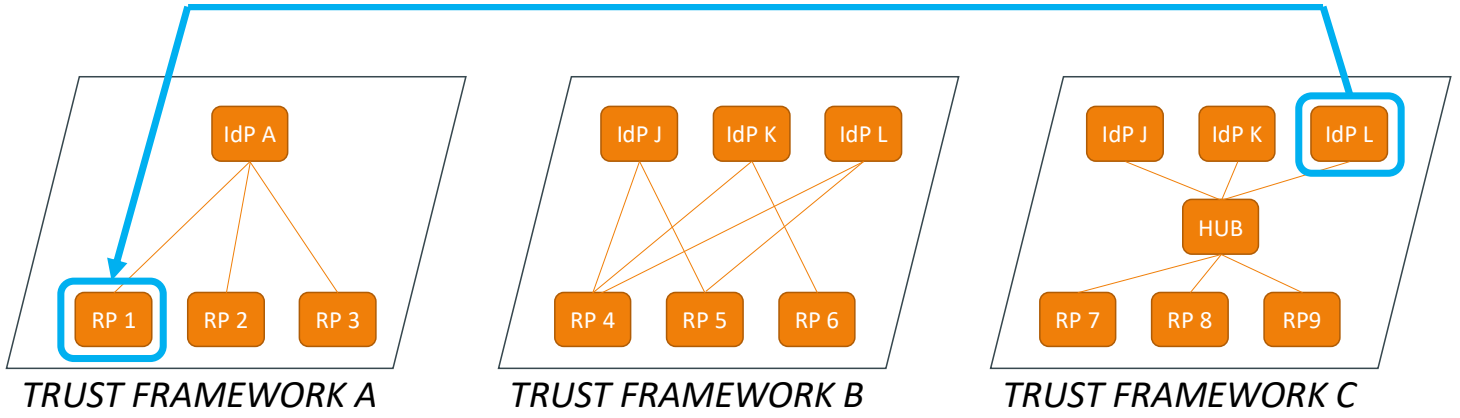
The working group recognised that a common understanding of the technical landscape is required to determine how digital identities could be used and recognised freely across countries. A universal set of definitions and taxonomies for digital identity will foster interoperability and allow for seamless collaboration between governments, private enterprise, and citizens.

Member countries also recognised that identity assurance and proofing requirements referencing open standards are important to enable mutual recognitions and establish a uniform baseline to support interoperability of digital identity systems. The survey identified that many DIWG members used broadly consistent identity assurance and proofing levels, including those based on ISO standards, National Institute of Standards and Technology (NIST) Electronic Authentication Guidelines and Identity Assurance Levels and Canadian Standards on Identity and Credential Assurance,

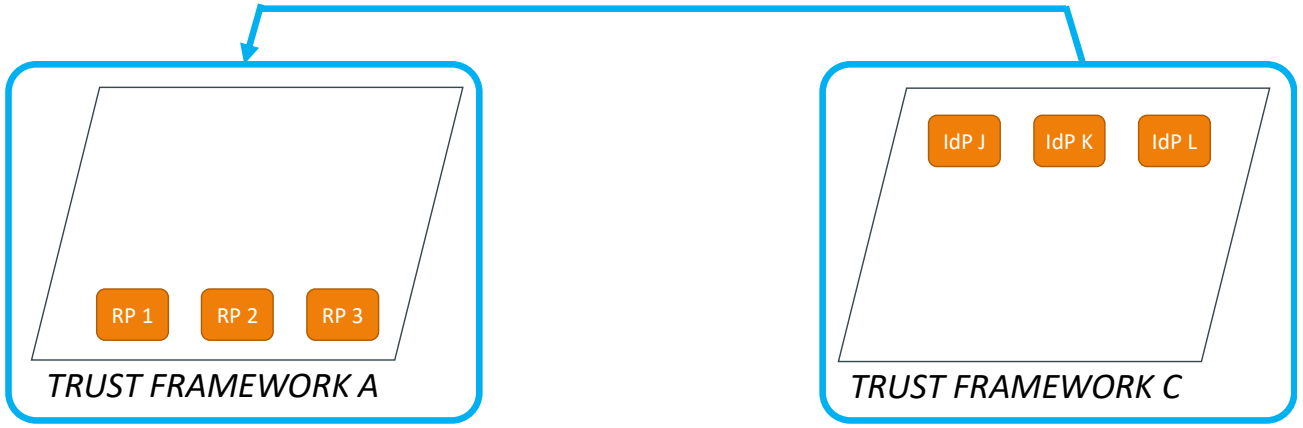


Level of Interoperability

✓✓✓✓

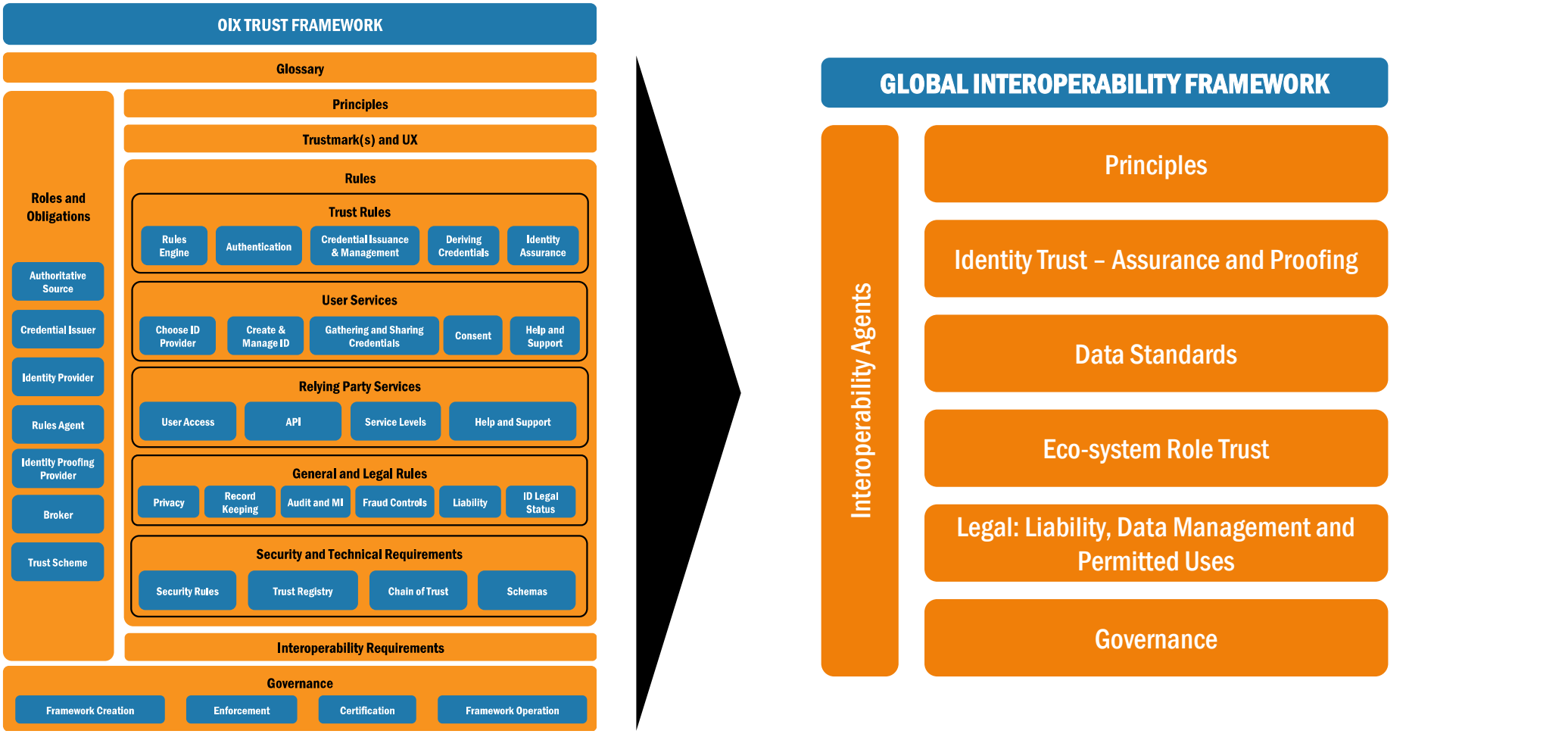


Peer to Peer



Framework to Framework

Global Interoperability Framework Key Requirements

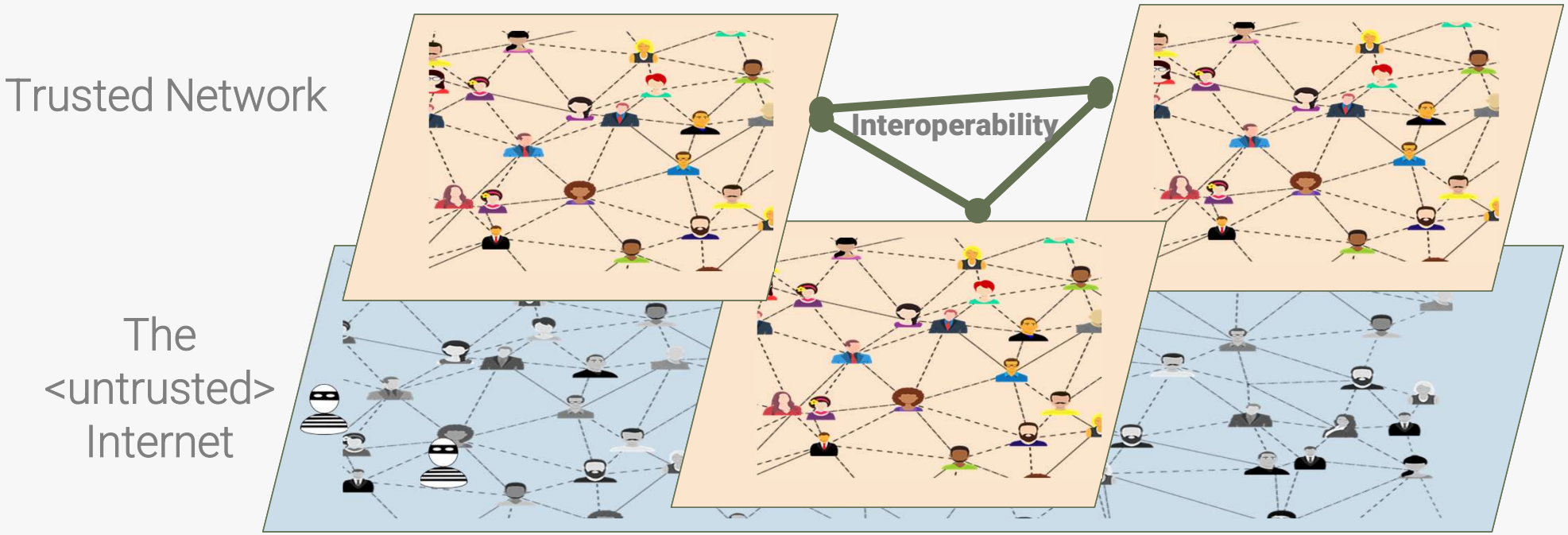


Global Interoperability Framework Principles

Principle	Description in the Context of Interoperability	DGX Principle
Reusability	Adoption (by both End-Users and Relying Parties) will depend upon End-User convenience. Interoperability frameworks ensure that End-Users re-use their established trusted Identity Information Providers, a familiar own language interface, and a simple process that connects them to services across the internet. A Trustmark shows the user, and organizations, that the interoperability framework is in operation.	Reusability Multilingualism
User Centricity	End-Users have control of their data. They may choose who they are shared with and how long for (purpose limitation). They also choose the Identity Information Provider involved. Transactions are always initiated by End-Users.	User Centricity
End-User Support	The user, and organizations relying on a Digital ID, must have somewhere to go when there is a problem and are guaranteed that their problem will be resolved promptly	
Transparency	The trust framework rules. operation and governance are open and clear to all parties.	Transparency
Technology Interoperability	Interoperability frameworks recognise technological diversity and are technology neutral. They may facilitate the integration of a variety of legacy infrastructures and identity solutions. The goal must be that oorganization's get consistent information about users regardless of which digital Identity Providers from which trust framework the user has chosen.	**Technology neutrality** and data portability
Data Interoperability	Data must be able to move and be reused access different systems.	Technology neutrality and **data portability**
Legal Interoperability	Interoperability frameworks should define the KEY rules that will needed to be codified in contracts that provide sufficient legal certainty as to participants' duties and obligations and ensure enforceability. They will also facilitate liability risk allocations and assessments as needed. Rules for data portability across frameworks should also be set. To ensure cross-border harmonization, these rules will be designed so as to minimize the applicability of certain existing legal and regulatory obligations in some jurisdictions.	
Identity Trust	Interoperability frameworks must allow a destination trust framework to understand trust in the credentials a user is presenting, facilitating the re-assessment of assurance policies to local rules if required. It must also enable the assessment of authenticators: are they robust enough for the destination trust frameworks policies? Records of trust must be delivered to, or be accessible by, organizations who rely on that trust in an integrity preserving manner.	Preservation of Information
Minimal Disclosure	Identity Information Providers share data directly with Relying Parties: Interoperability frameworks ensure only appropriated parties have access to End-User Data. Furthermore, Relying Parties can request only the minimum required for their use case. End-Users will have control over whether to share each attribute.	Openness
Eco-System Actor Trust	Interoperability frameworks must ensure that all in parties are real, identifiable, and can be held accountable for their actions. As such, authentication and identification of all parties is always required when interacting from framework to framework.	
Fraud	Digital IDs are protected from fraud by trust frameworks. Consequences of fraudulent IDs are understood and catered for in legal agreements.	
Inclusion	All users who choose to do so can leverage their Digital ID in interoperable trust frameworks.	Inclusion and Accessibility
Administrative Efficiency	Interoperability Frameworks should simplify the operation of Digital IDs across frameworks, preferably by achieving multi framework interoperability.	Administrative Simplicity Effectiveness and Efficiency

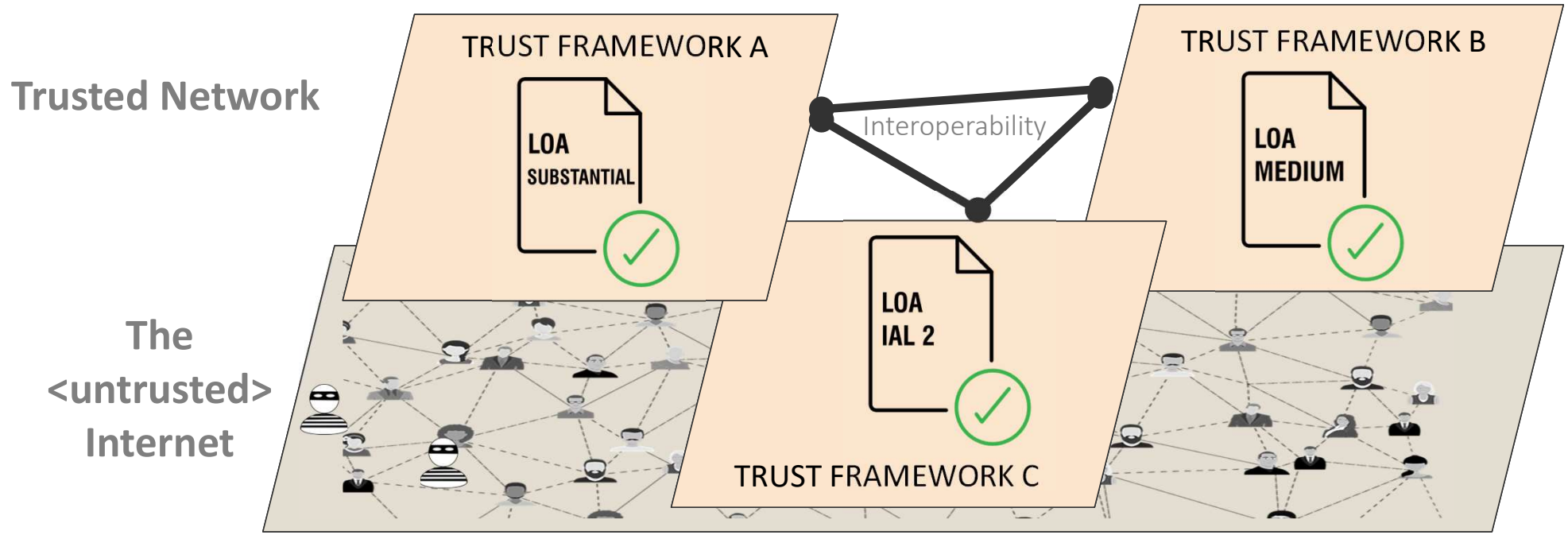
GAIN Vision

Islands of trust exist, GAIN is an interoperable system bridging islands



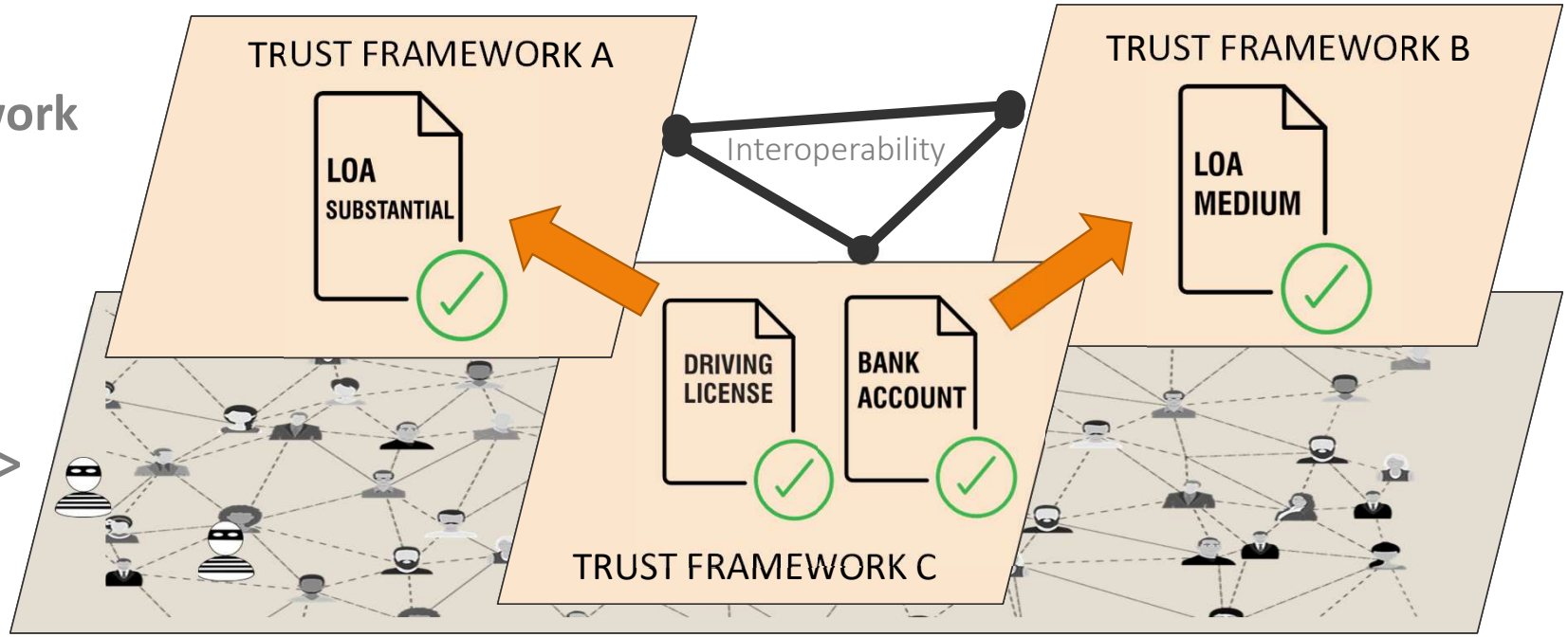
Identity Trust – Assurance and Proofing
The Currency of Identity

Is a **Level of Assurance** interoperable?

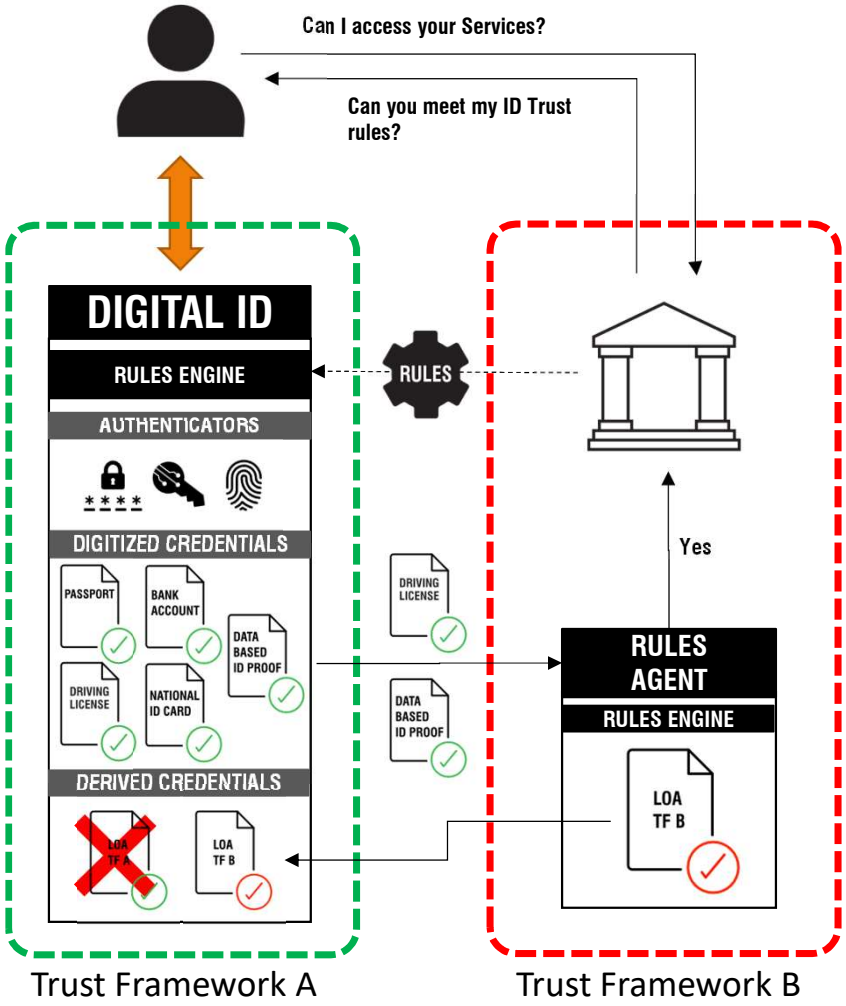


Identity Trust – Assurance and Proofing
The Currency of Identity

Or must we revert to Trust Framework **assured Digitized Credentials** to assess a local Level of Assurance?



Example: Deriving a locally acceptable LoA credential

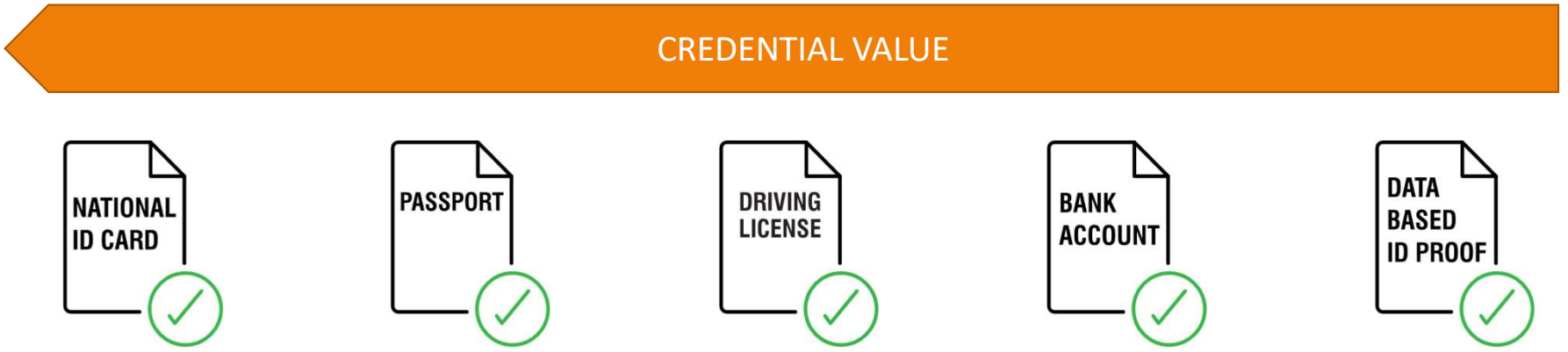


- A 'Rules Agent' within the destination trust framework, with the users consent, creates the required Level of Assurance credential.
- The Rules Agent would be appointed by and operate to the rules of Trust Framework B.
- The resultant Assured Credential can be stored in the users Digital ID within Trust Framework A for re-use with other RPs in Trust Framework B.
- It's Chain of Trust flows to Trust Framework B and back to Trust Framework As original Proofed Credentials.

Identity Trust – Assurance and Proofing
The Currency of Identity

If we are to trade in Digitized Credentials, do we need **global standards** for them?

Are some Digitized Credentials 'worth more' than others?



Local approach, but government backed

Global ICAO standard

mDL standard (but not for user verification on digital issuance)

Banks all work to AML standards

Local Standards

Data Standards

OIX Architecture Interoperability Working Group

Naming: a mixed bag of standards!

Naming: New standards in OIDC for ID Assurancev

	Claims	Evidence	Proofing	Assurance
CORE ID INFORMATION	Core ID Claims • Name • Address • DoB • Nationalities • Contact Details • Personal Identifiers	ID Documents • National ID • Passport • Driving License Electronic Records • Bank Account • CRA Check • Electoral Roll • Fraud Check • Mortality Vouches • Via Digital ID • Face to Face	Validation Methods: • Face to Face • Scanning • API Call using self declared data Verification Methods: • KBVs • OTCs • Selfie Cross Matches • Face to Face Activity Methods • Electronic Activity Evidence • Vouched Activity ID Fraud Methods: • Known Fraud • Risk Signal	Trust Framework Assurance Level Assurance Policy Assurance Procedure Assurance Elements and Scores: • Strength / Validation • Activity • ID Fraud • Verification Mapping Elements Scores back to Evidence

Key:

Too Many Standards

Local Standards

Global Standards

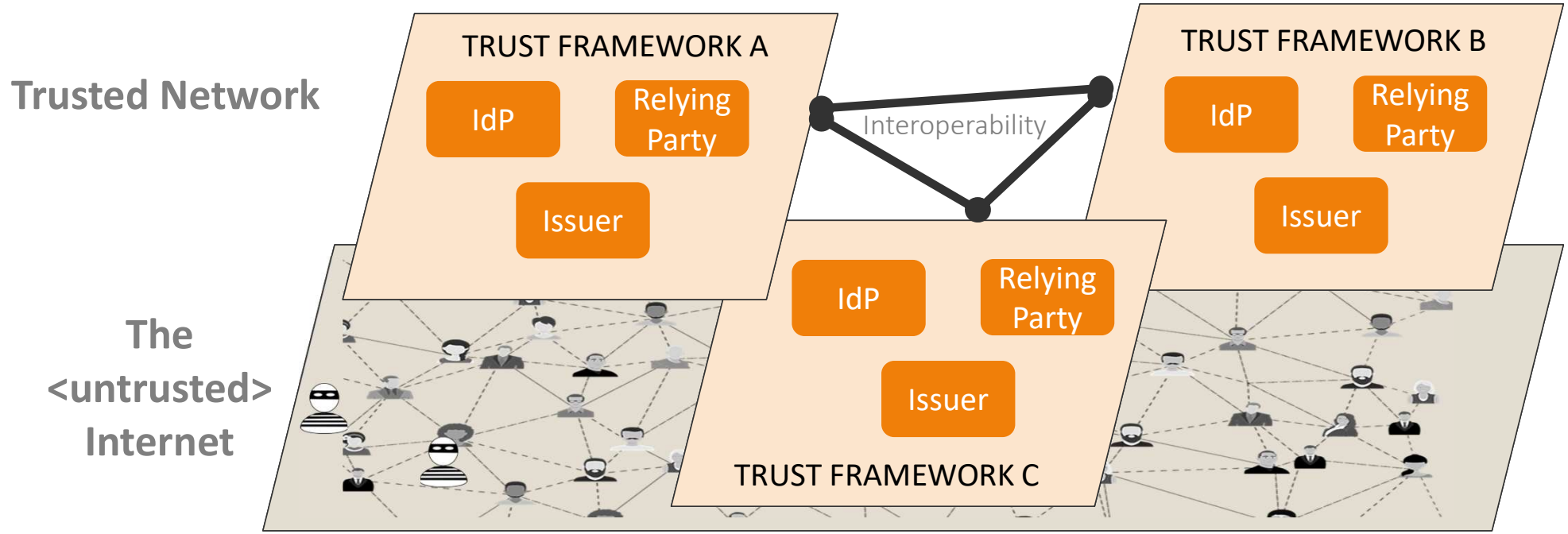
No Standards

Proofing Process: Trust Framework level standards. Emerging ISO, NIST, ESTC stsnards

Assurance Process: Similar Approaches Across trust frameworks,

Ecosystem Role Trust

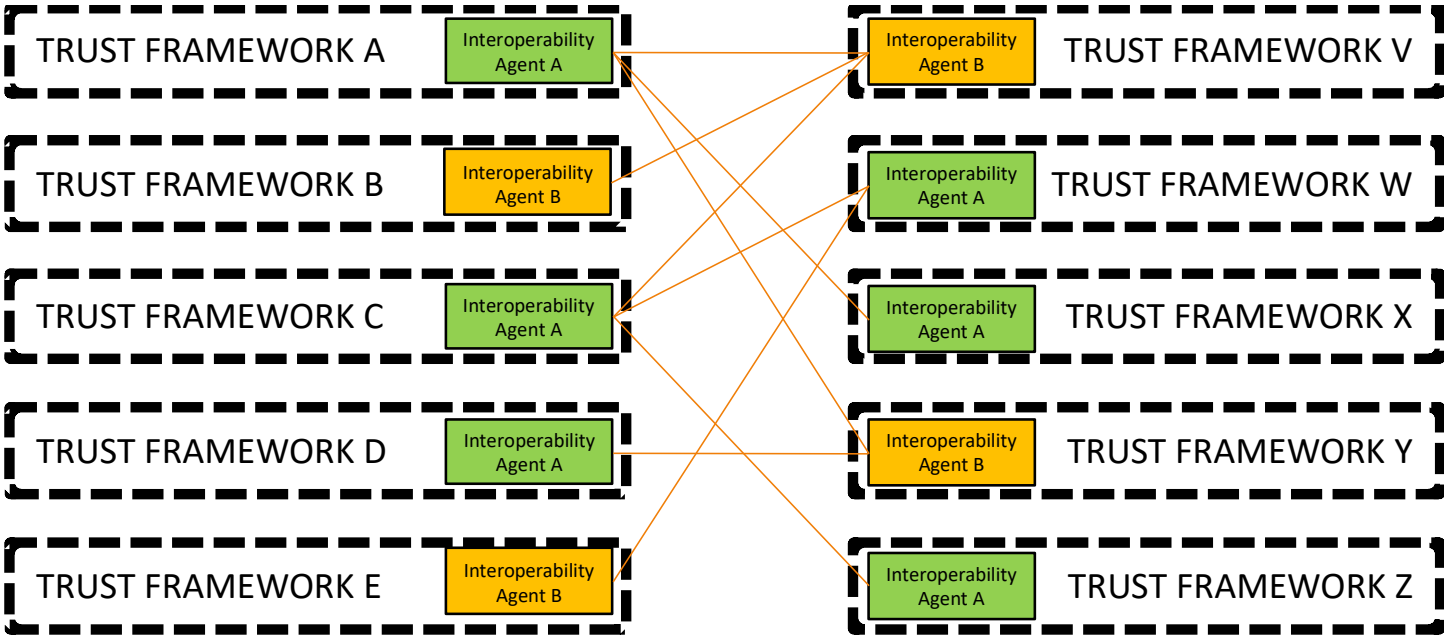
Can we standardize Roles for interoperability?
Who is authorized to play what role? What can they do?
How do frameworks govern onboarding of roles?



Legal: Data Protection, Permitted Uses and Liability

	Issuer	IdP	Relying Party
DATA PROTECTION		Is user consent captured in a way the meets the target frameworks needs?	Is data managed in a way the meets the releasing frameworks needs?
LIABILITY	Is any party liable for an incorrect or fraudulent Identity? Government Vs Private Sector frameworks		
PERMITTED USES	Are there any restrictions on where and by whom a credential can be used?		

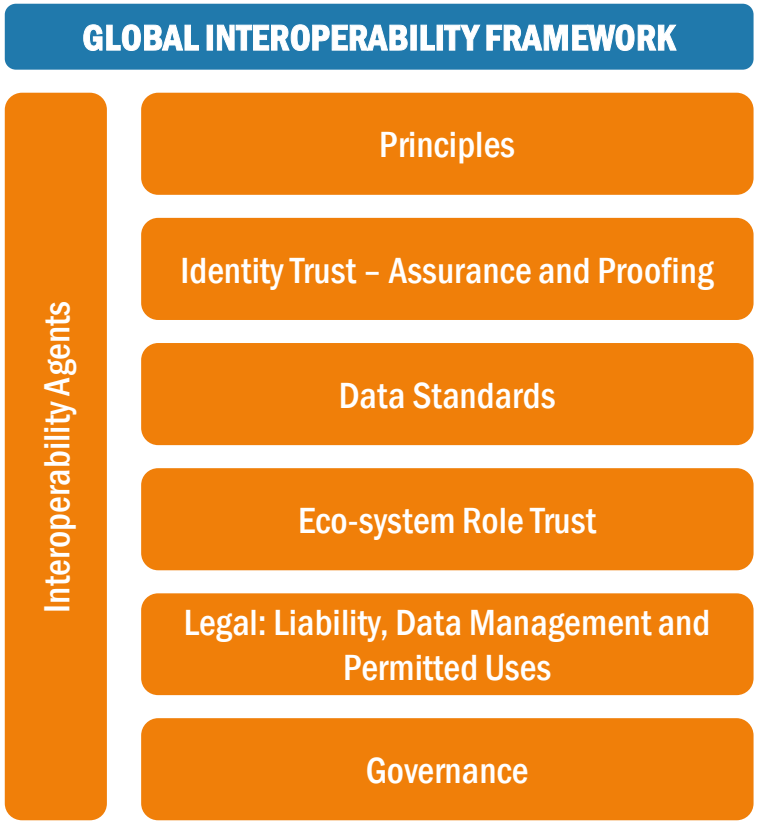
Do we need a new Role? – Interoperability Agent?



Interoperability Agents might:

- Overlay Role Standards
- Overlay Proofing Standards
- Overlay local Levels of Assurance
- Broker cross framework Level of Assurance acceptance
- Overlay liability cover
- Overlay common policies for: authenticators, data management &permitted uses
- Provide Commercial Services: contracts, billing, reconciliation

Next Steps



- We have only just begun!
- We will continue to explore the requirements for a Global Interoperability Framework over the next few months
- A part of this will be analysis of existing Trust Frameworks
- We have completed an initial desk top analysis of Trust Frameworks:
  - Analysis shows expected similarities between frameworks
  - Different elements of different frameworks are transparent
- Need to work with Trust Frameworks as part of this process
  - We invite trust frameworks to work with us on the Global Interoperability Framework requirements

Join us

Global Interoperability
OIX WG

OPEN IDENTITY EXCHANGE

openidentityexchange.org

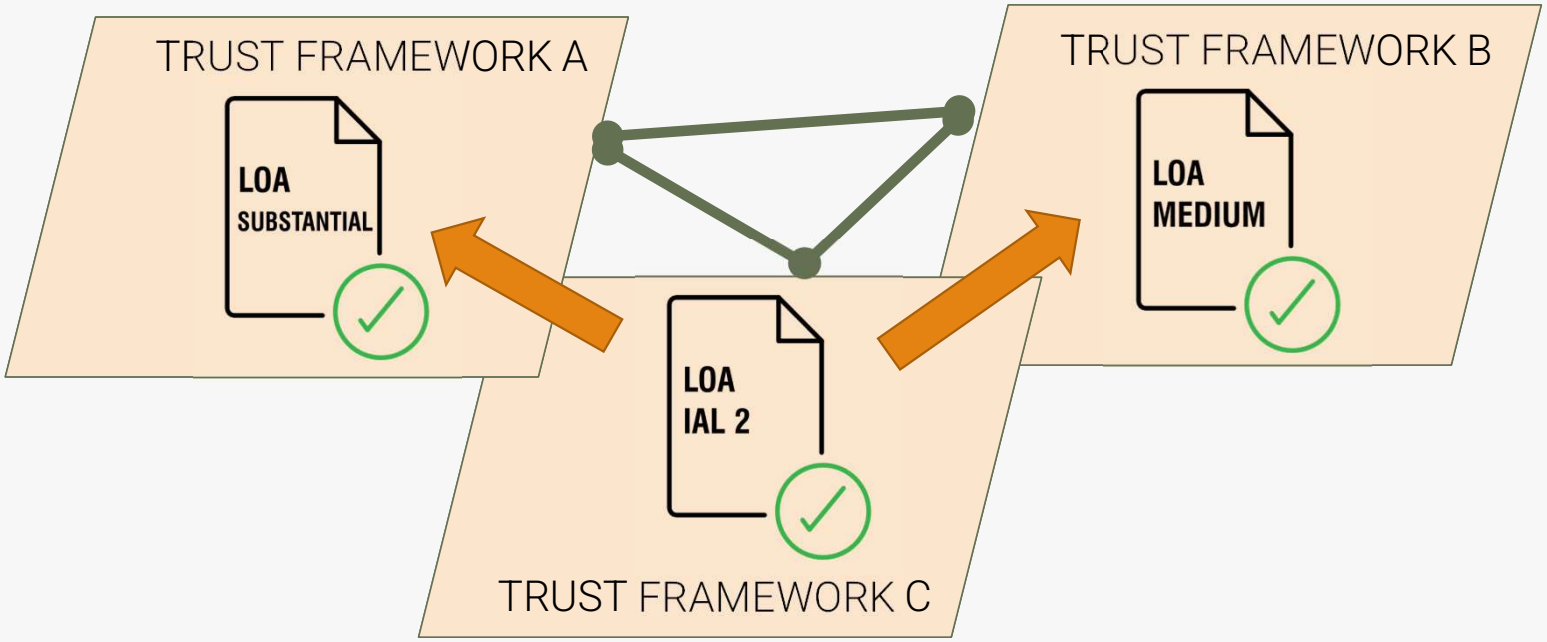
To learn more about the GAIN POC Community Group, join the conversation GAINPOC@oidf.org or connect on LinkedIN

To learn more or get involved in OI standards visit www.openid.net

GAIN POC

OpenID

Is a Level of Assurance interoperable?



Or must we revert to Trust Framework **assured Digitized Credentials** to assess a local Level of Assurance?