OIX 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, Digidentity, Digital 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

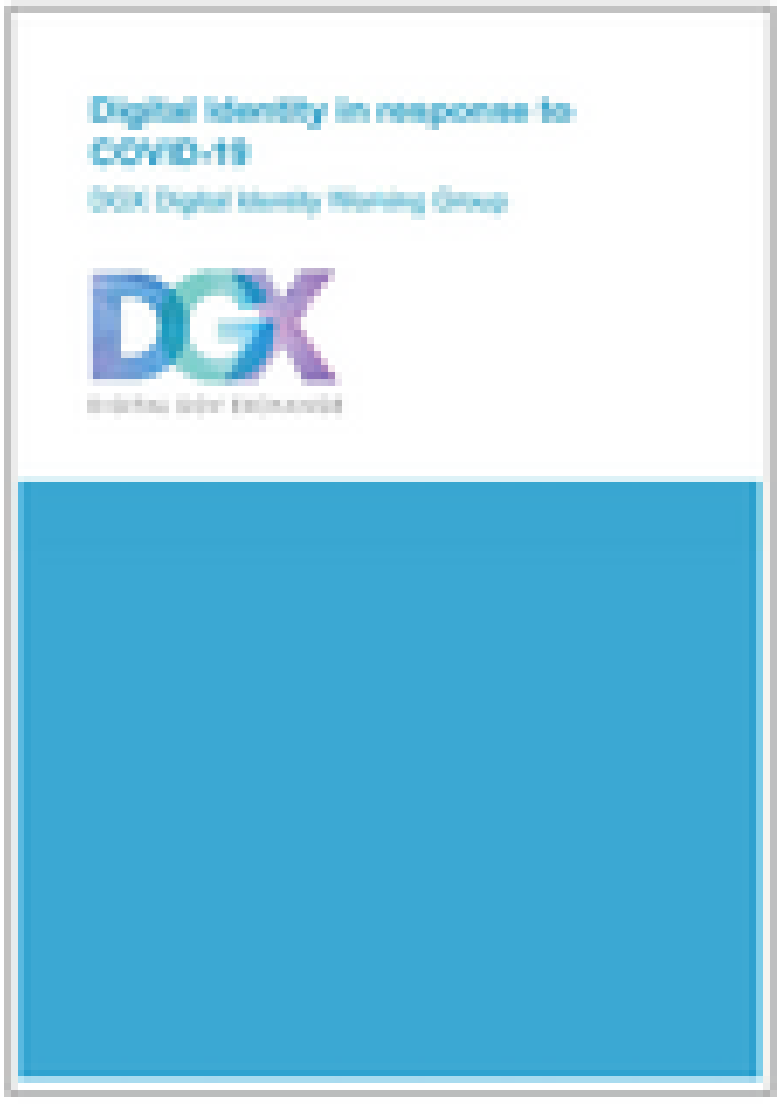
[illegible]

[illegible]

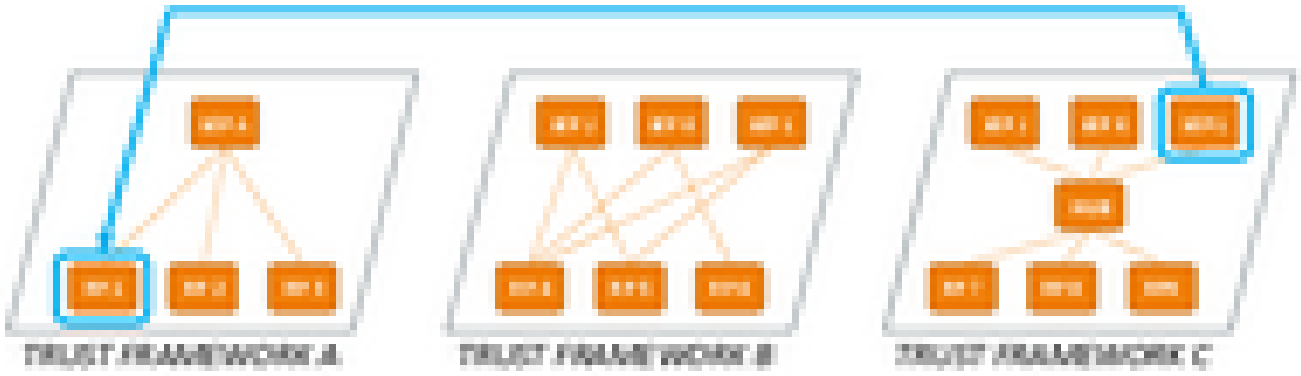
[illegible]

[illegible]

[illegible]



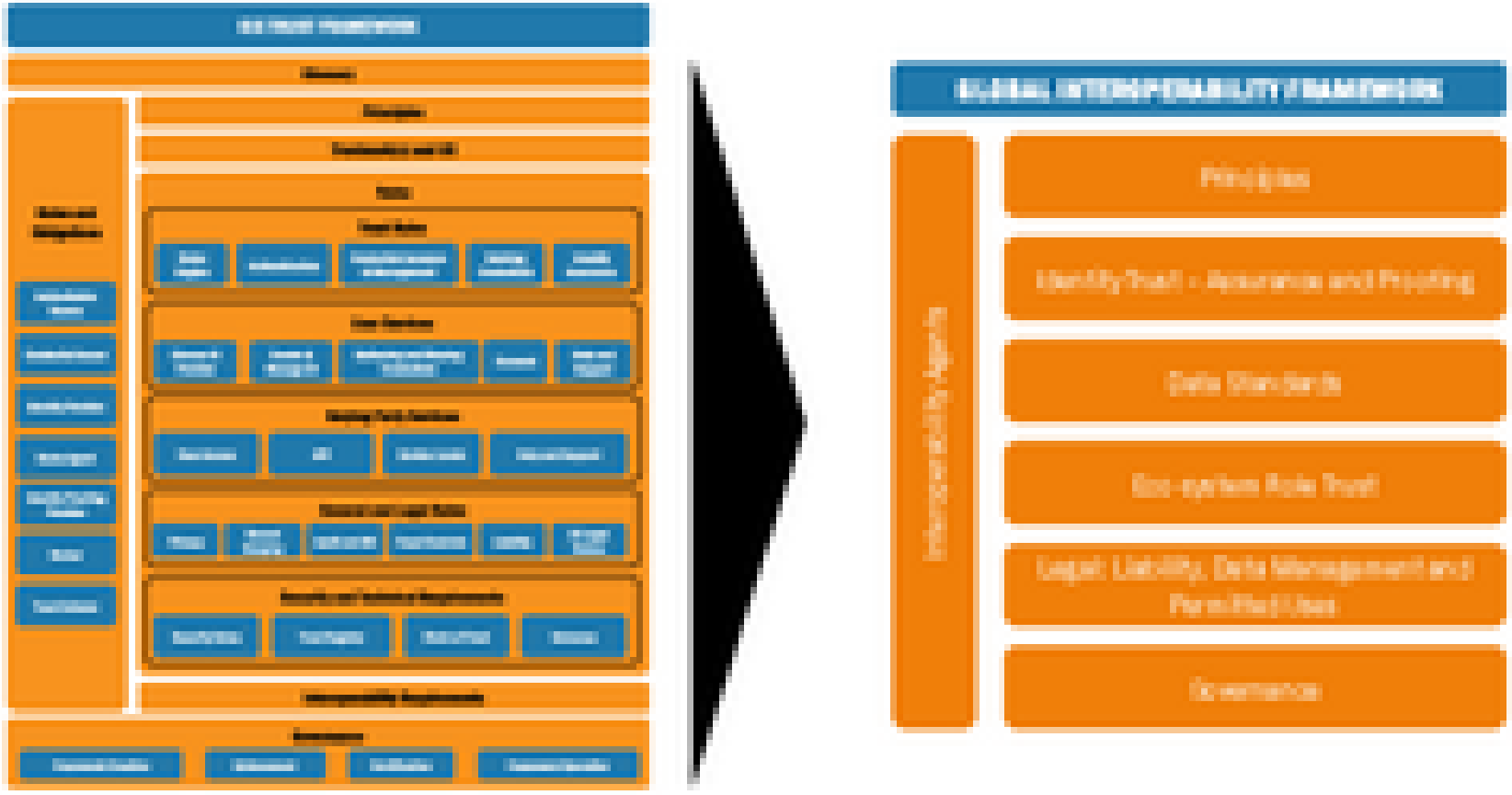
Level of Interoperability



Peer to Peer

Framework to Framework

Global Interoperability Framework
Key Requirements

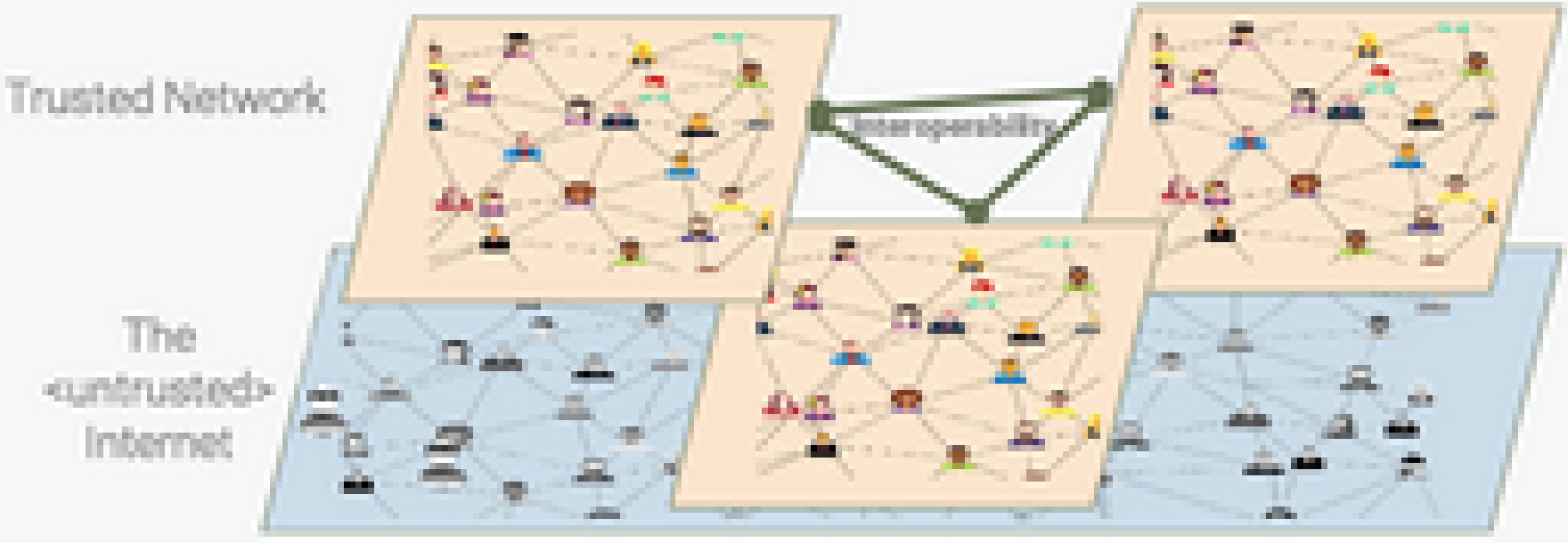


Global Interoperability Framework Principles

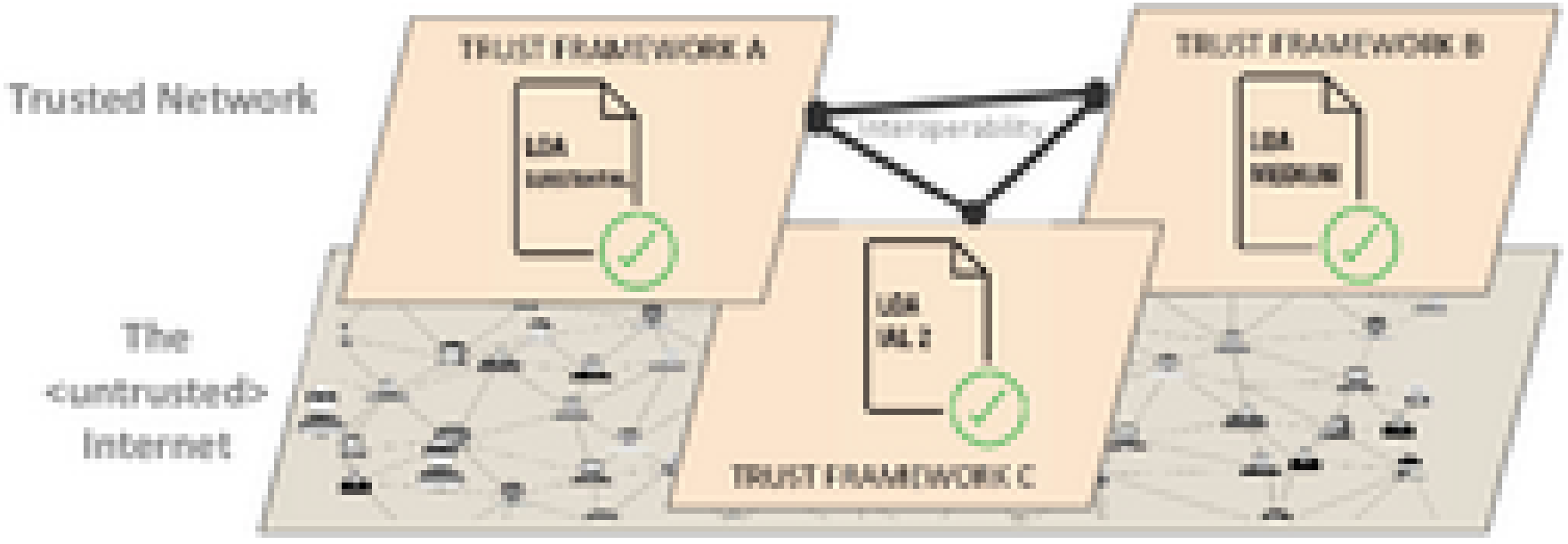
Principle	Description in the Context of Interoperability	DIX Principles
Reusability	[illegible]	[illegible]
User Centricity	[illegible]	[illegible]
End-User Support	[illegible]	
Transparency	[illegible]	[illegible]
Technology Interoperability	[illegible]	[illegible]
Data Interoperability	[illegible]	[illegible]
Legal Interoperability	[illegible]	
Identity Trust	[illegible]	[illegible]
Minimal Disclosure	[illegible]	[illegible]
Sys-System Actor Trust	[illegible]	
Broad	[illegible]	
Inclusion	[illegible]	[illegible]
Administrative Efficiency	[illegible]	[illegible]

GAIN Vision

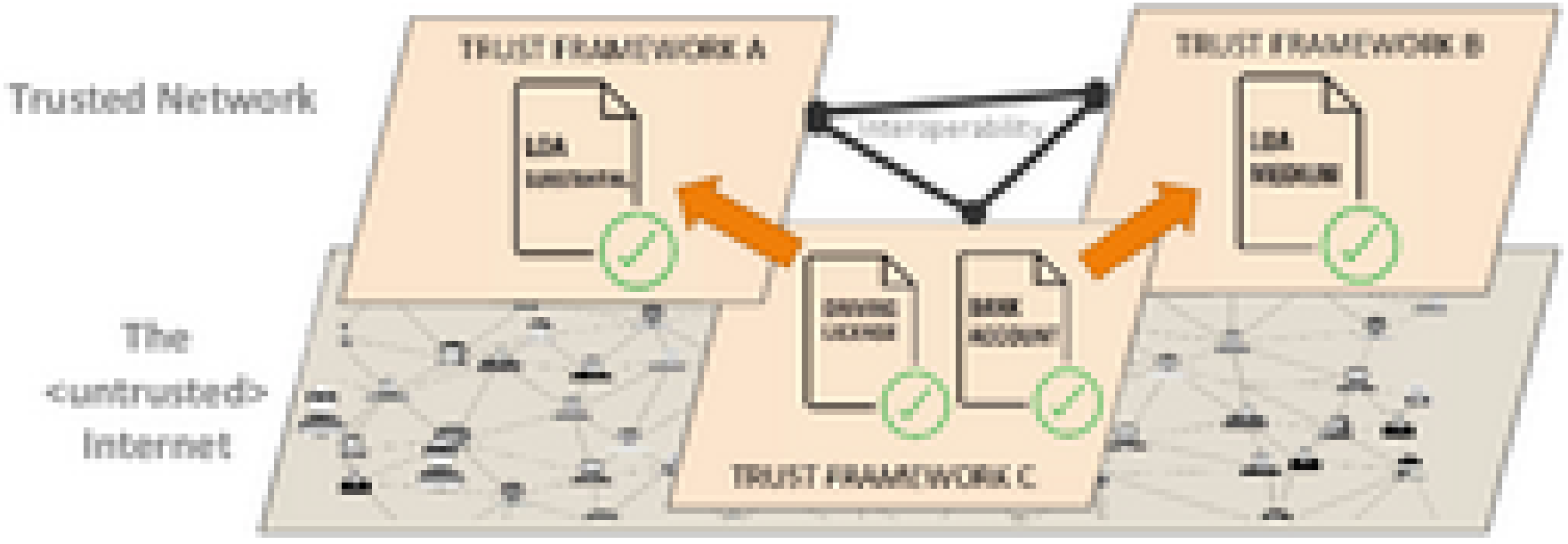
Islands of trust exist, GAIN is an interoperable system bridging islands



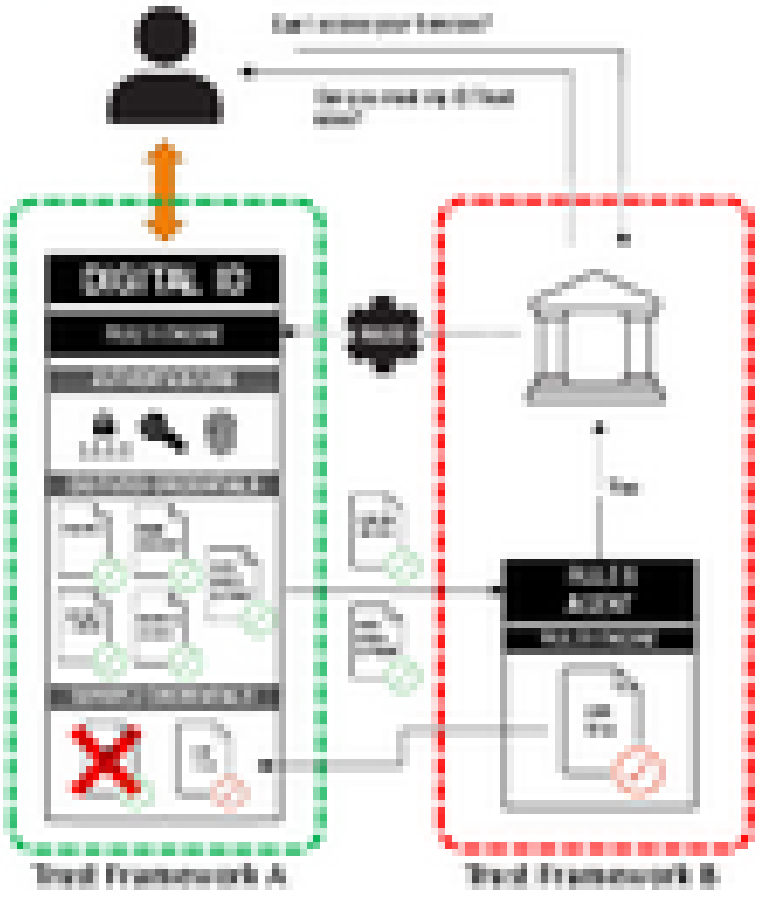
Is a **Level of Assurance** interoperable?



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



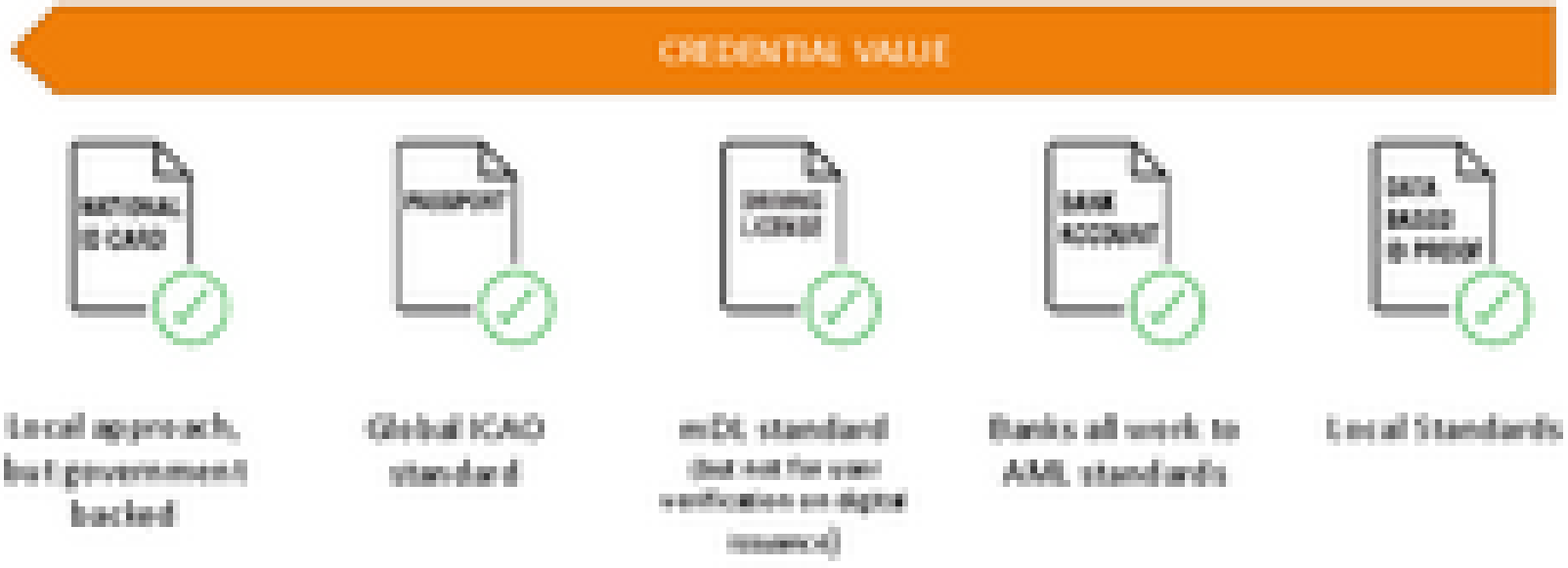
Example: Deriving a locally acceptable LoA credential



- 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 A's 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?



Data Standards

OIX Architecture Interoperability Working Group

Naming: a mixed bag of standards!

Naming: New standards in OIDC for ID Assurance

	Claims	Evidence	Proofing	Assurance
OIX PIC ID (NFI DIGIT ATION)	Core ID Claims • Name • Address • DoB • Nationalities • Contact Details • Personal Identifiers	ID Documents • National ID • Passport • Driving Licence Electronic Records • Bank Account • DRA Check • Electoral Roll • Fraud Check • Mortality Vouches • Via Signal ID • Face to Face	Validation Methods • Face to Face • Scanning • API Call using self declared data Verification Methods • KBVs • OTCs • Selfie Check Matches • Face to Face Activity Methods • Electronic Activity Evidence • Vouched Activity ID Fraud Methods • Known Fraud • Anti 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

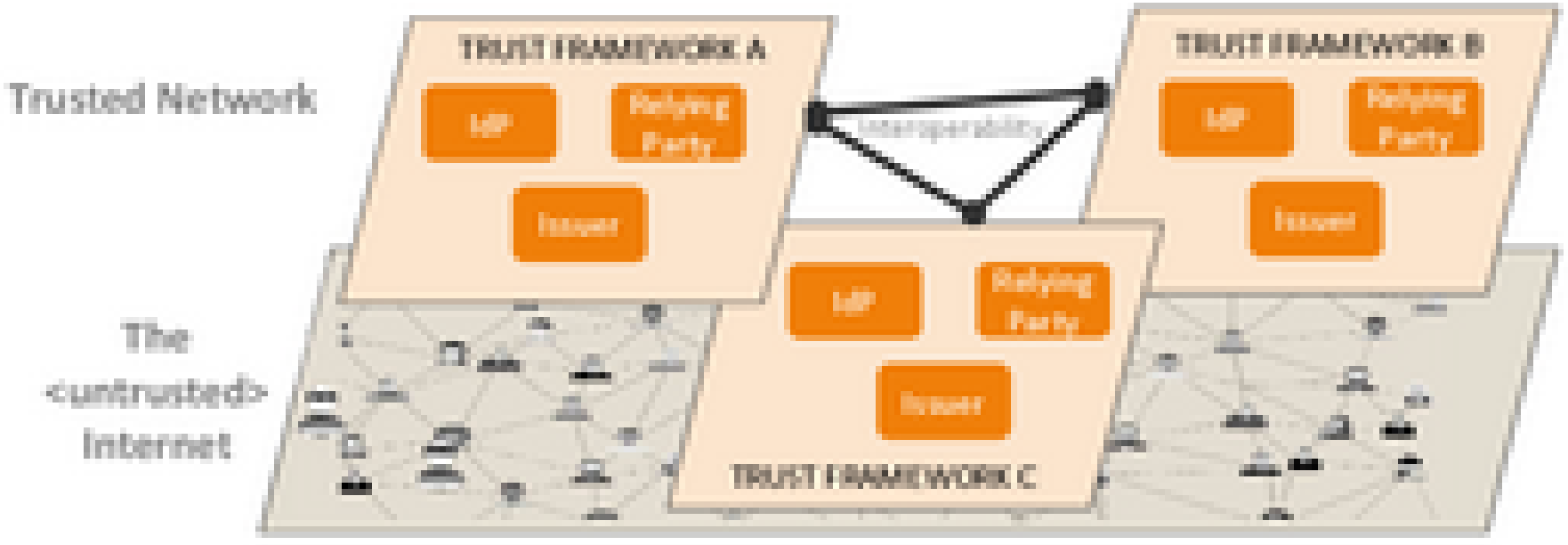
Global Standards — No Standards

Proofing Process
Trust Framework
level standards
Emerging ISO, NIST
OIDC standards

Assurance Process
Similar Approaches
Across trust
frameworks

Ecosystem Role Trust

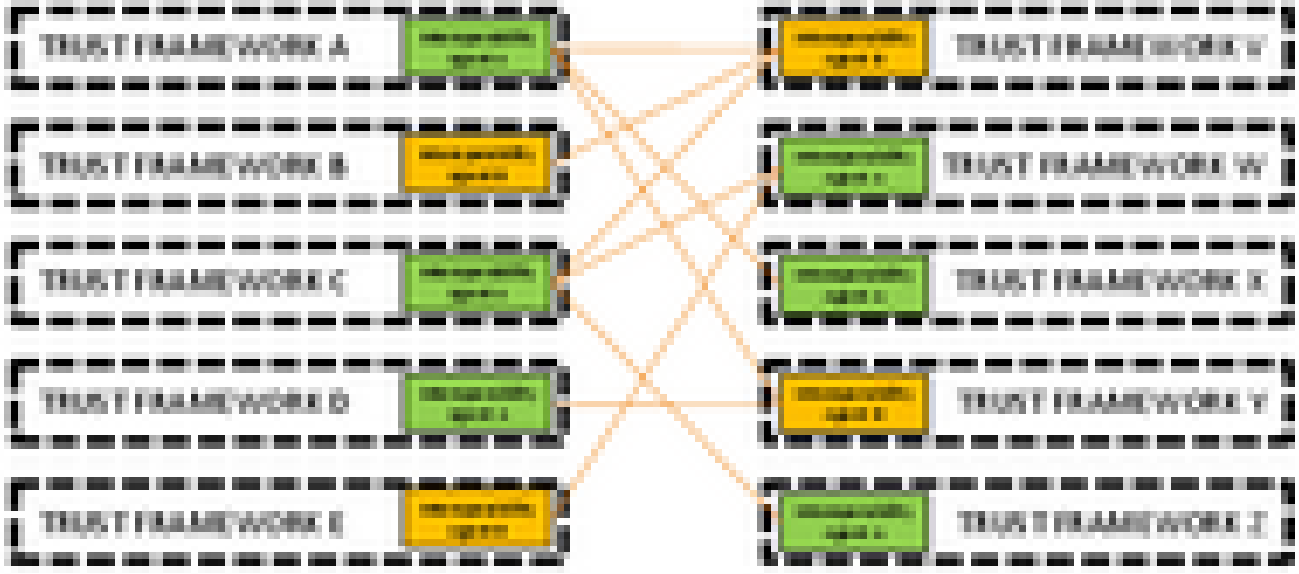
Can we standardize Roles for interoperability?
Who is authorized to play what role? What can they do?
How do frameworks govern onboarding of roles?



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

OIX OPEN IDENTITY EXCHANGE

openidentityexchange.org

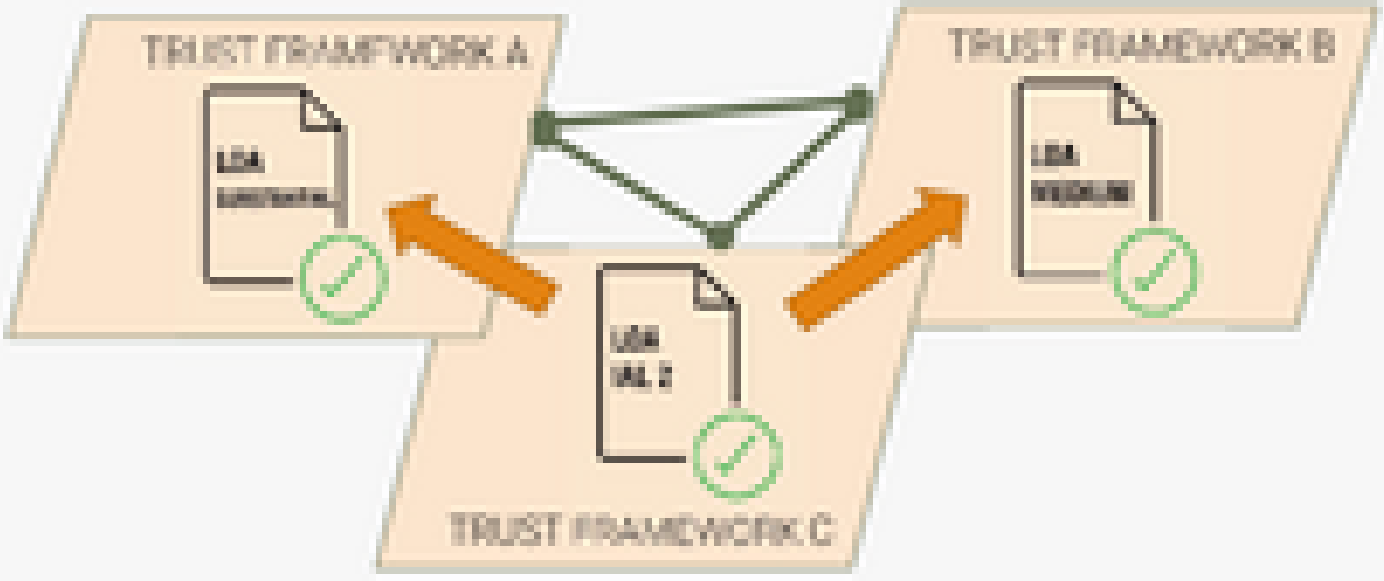
To learn more or get involved in OI
standards visit www.openid.net

GAIN POC

OpenID

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

Is a **Level of Assurance** interoperable?



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