



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 be 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, GLIEDF, Hooyse, 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 Interoperability

However, the working group recognised that both digital recognition and interoperability are complex challenges that will take several years to achieve. These require policy, legal and technical alignment between government and businesses, public institutions, and individuals. Efforts to create interoperability, such as the EU's ARISE, show these challenges are significant to overcome.

The DGX identified **additional activities** focused to enable both digital recognition and interoperability of right assertions, including:

1. The definition of a common language and definitions across digital identities
2. Assessment and alignment of respective legal and policy frameworks, interoperability, appropriate consensus on identity standards and cross-border application, and
3. Interoperable technical models and infrastructures

However, differences in legislation and specific government requirements may also impact mutual recognition and interoperability. This includes issues such as offering choices or a single digital identity, privacy and personal data regulation, security standards, interoperability across borders, and the role of government and the private sector in digital identity systems.

This working group recognised that a common understanding of the outcome of interoperability is required to enable effective digital identities across the credit and insurance finance sectors. In addition, a common set of standards and framework for digital identity, **ID4All**, interoperability and other forms of cross-border collaboration between governments, private enterprises, and citizens.

Member countries also recognised that identity transparency and profiling requirements, following open standards are important to create robust recognition and validation. A common objective is support interoperability of digital identity systems. The survey identified the major EU member's most closely aligned security measures and profiling factors including those based on ISO documents, National Institutes of Standards and Technology (NIST) practices, Authentication (Individual and Identity Assurance Levels and Certified Transactors or Identity User Credential Assurance).

Digital Identity in response to COVID-19

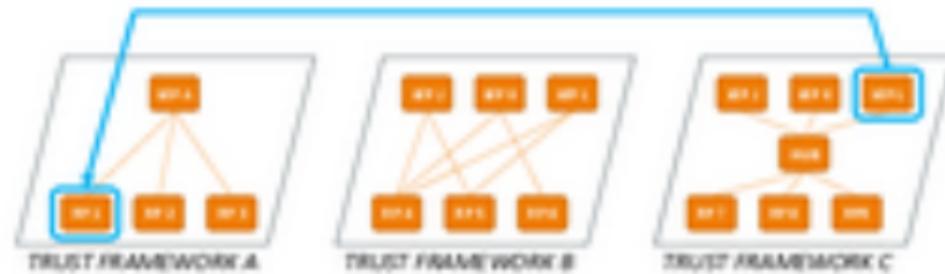
DGX Digital Identity Working Group



Level of Interoperability

4/4/4

Peer to Peer



Framework to Framework



Global Interoperability Framework Key Requirements

OIX



Global Interoperability Framework Principles



Principle	Description in the Context of Interoperability	SDG Principle
Accessibility	Interoperable systems must be designed to be accessible to people with disabilities. This includes the provision of assistive technologies such as screen readers, keyboard navigation, and multiple input methods. Accessibility must be built-in from the earliest stages of system development.	SDG 10.1.1
User Experience	User experience must be considered throughout the design process. The user interface must be simple, intuitive, and accessible. Feedback loops must be included in the design process.	SDG 10.1.2
Environment-Support	The design of interoperable systems must support environmental sustainability and reduce the impact of the system on the environment.	SDG 12.1.1
Transparency	The mechanisms used to support transparency must be transparent and explainable.	SDG 12.1.2
Technology Interoperability	Interoperable systems must support technology neutrality and use open standards. They must be able to integrate with a variety of legacy information and data sources. They must be able to support different communication protocols and data formats.	SDG 12.1.3
Data Interoperability	Interoperable systems must support data exchange between different systems.	SDG 12.1.4
Legality Interoperability	Interoperable systems must be designed to be compliant with relevant legal requirements, including copyright laws, data protection regulations, and privacy laws. They must be able to handle sensitive data and ensure its security.	SDG 12.1.5
Security Trust	Interoperable systems must be designed to be secure, protecting data and systems from cyber threats, viruses, and other malicious attacks.	SDG 12.1.6
Minimal Bottlenecks	Interoperable systems must be designed to minimize bottlenecks, ensuring smooth data flow and efficient system performance.	SDG 12.1.7
One-System-Accelerator	Interoperable systems must be designed to accelerate the development of one system, reducing the time required for system integration.	SDG 12.1.8
Read	Interoperable systems must support reading functionality, allowing users to extract and interpret data from the system.	SDG 12.1.9
Iteration	Interoperable systems must support iterative development, allowing for continuous improvement and refinement.	SDG 12.1.10
Administrative Efficiency	Interoperable systems must support the automation of administrative tasks, reducing administrative overhead.	SDG 12.1.11

GAIN Vision

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

Trusted Network

The
<untrusted>
Internet

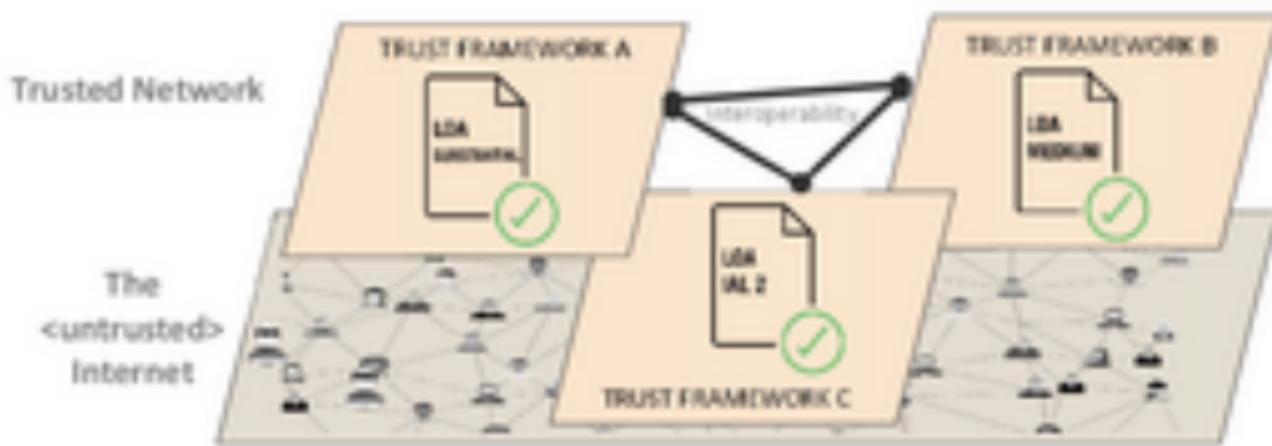


Identity Trust – Assurance and Proofing

The Currency of Identity

oix

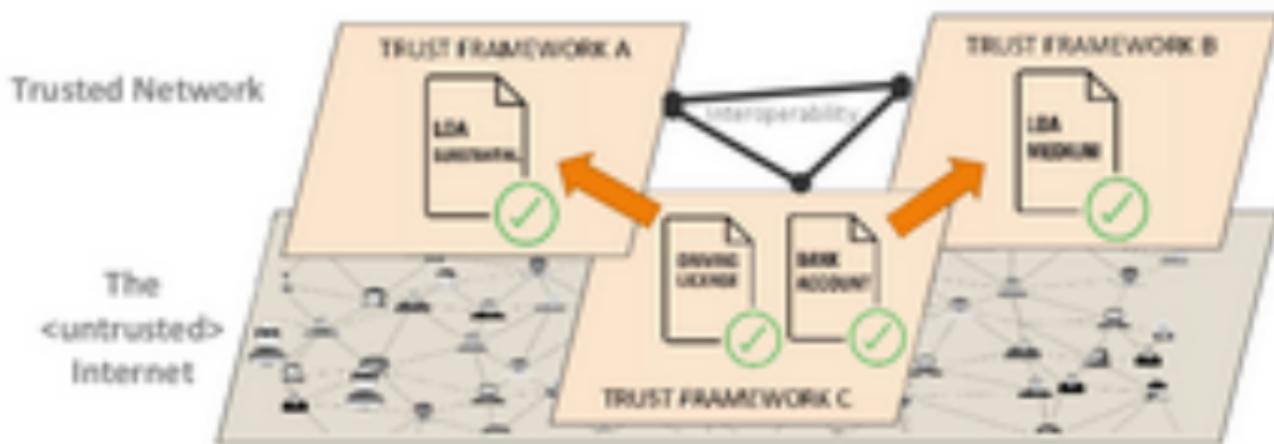
Is a Level of Assurance interoperable?



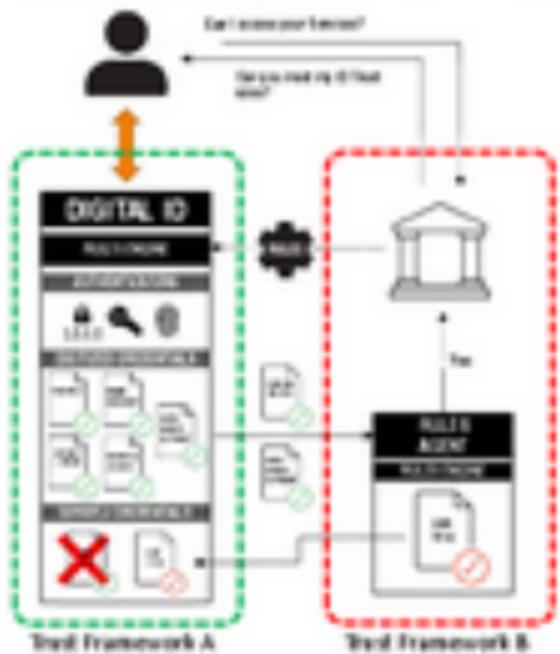
Identity Trust – Assurance and Proofing The Currency of Identity

oix

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 Protected 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?

CREDENTIAL VALUE



Local approach,
but government
backed



Global ICAO
standard



eID, standard
(but not for user
verification or digital
signature)



Banks all work to
AML standards



Local Standards

Data Standards

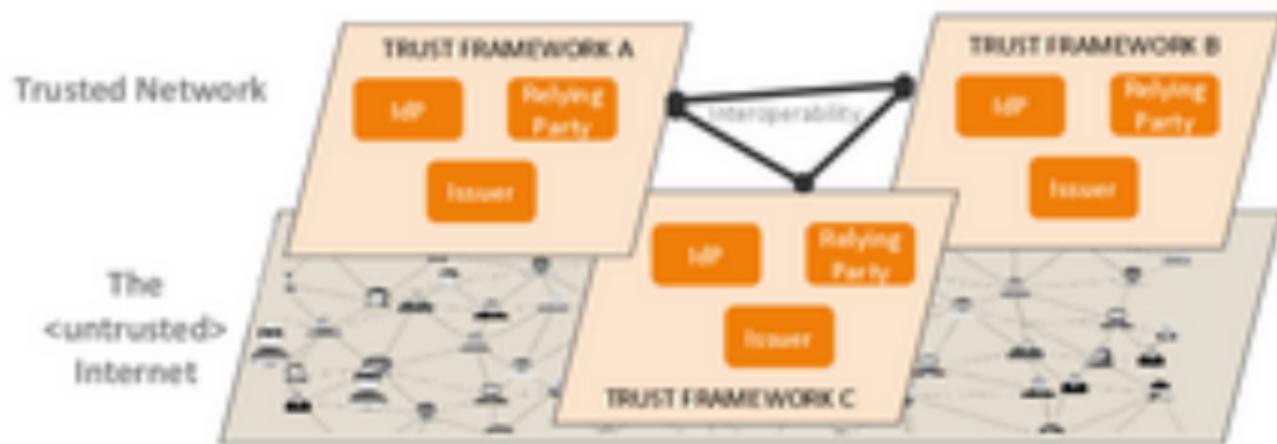
OIX Architecture Interoperability Working Group



	Naming: a mixed bag of standards	Naming: New standards in ODC for ID Assurance
Current	Business	Assurance
Same as ID providers	<ul style="list-style-type: none"> • Business • National ID • Passport • Driving license <p>ODC ID Details</p> <ul style="list-style-type: none"> • Name • Address • Date • Nationality • German Details • Personal Identifier <p>Electronic Records</p> <ul style="list-style-type: none"> • Bank Account • ODA/ODC • Insurance Bill • Fraud Check • Identity <p>Witness</p> <ul style="list-style-type: none"> • Video Signal ID • Face to Face 	<p>Verification Methods:</p> <ul style="list-style-type: none"> • Face to Face • Scanning • API/Calling off standard lists <p>Verification Methods:</p> <ul style="list-style-type: none"> • IRIS • OTTO • Self-Declaration • Face to Face <p>Activity Methods:</p> <ul style="list-style-type: none"> • Electronic Activity Evidence • Visualized Activity <p>ODC Fraud Methods:</p> <ul style="list-style-type: none"> • Known Fraud • Suspicious
	<p>Key:</p> <p>Too Many Standards Global Standards</p> <p>Local Standards No Standards</p>	<p>Assurance Process</p> <p>Strong Framework Local standards Emerging ODI, NIST, FIDO standards</p> <p>Assurance Process</p> <p>Similar Approaches Across Work Frameworks</p>

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



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



openidentityexchange.org

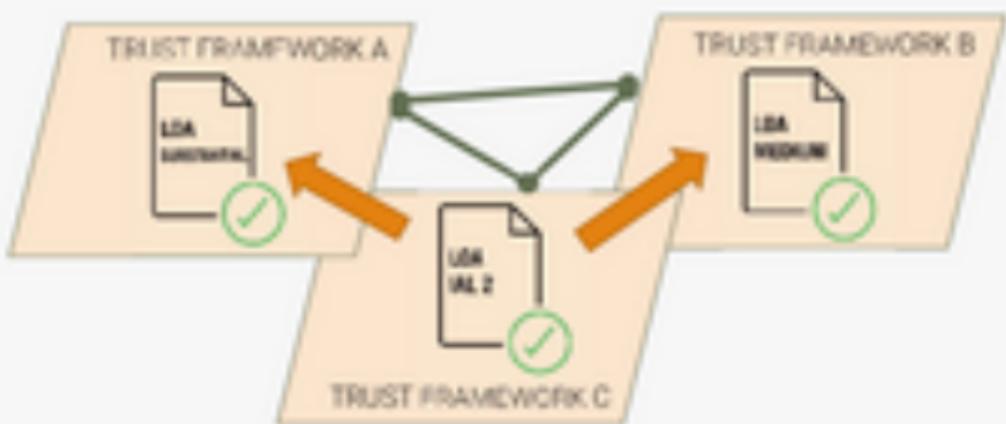
To learn more about the GAIN POC
Community Group, join the conversation
GAINPOC@openid.net or connect on
LinkedIn

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

GAIN POC



Is a Level of Assurance interoperable?



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

