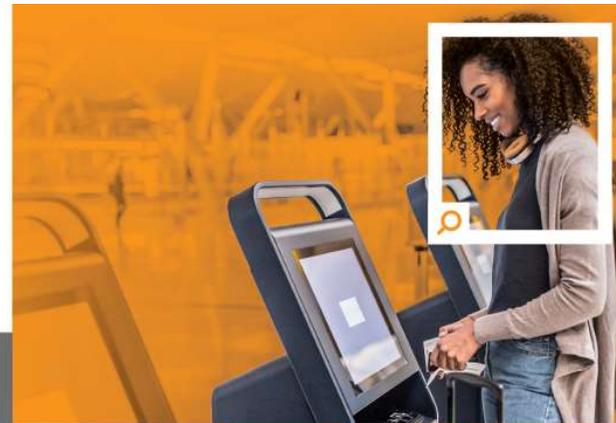




# Making Digital ID a Success

## Workshop

29<sup>th</sup> March 2022



# Agenda



- 12.30 **Registration** - Tea/Coffee will be served
- 13.00 **Introduction & Welcome** - *Nick Mothershaw, Chief Identity Strategist*
- 13.05 **The Road to EIDAS 2.0 Payment Wallets** - *Michael Adams, payments consultant & founder of Quali-Sign,*
- 13.35 **Understanding the Human Impact of ID Exclusion** - *Dr Sarah Walton, ID Code of Conduct Programme Manager, Women in Identity*
- 14.05 **The UK Online Safety Bill and euCONSENT** - *Iain Corby - Age Verification Providers Association*
- 14.35 **OIX Strategy Update** - *Nick Mothershaw, OIX Chief Identity Strategist*
- 14.50 **Member Update** - Emma Shaw, OIX Member Manager
- 14.55 **Wrap Up**
- 15.00 **CLOSE**



Making Digital ID a Success

## The Road to EIDAS 2.0 Payment Wallets

*Michael Adams, payments consultant & founder of Quali-Sign*





Making Digital ID a Success

# Understanding the Human Impact of ID Exclusion

*Dr Sarah Walton, ID Code of Conduct Programme Manager, Women in Identity*

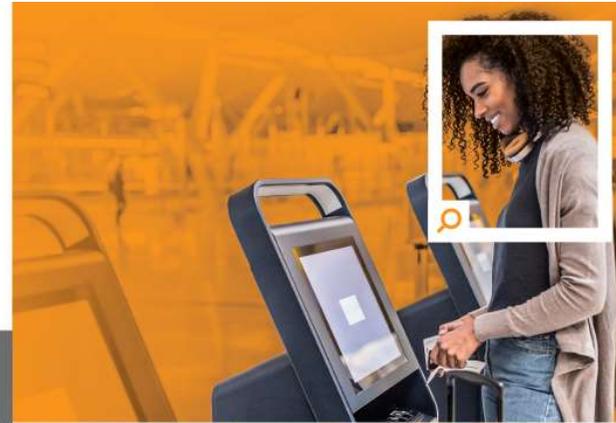




Making Digital ID a Success

# The UK Online Safety Bill and euCONSENT

*Iain Corby - Age Verification Providers Association*



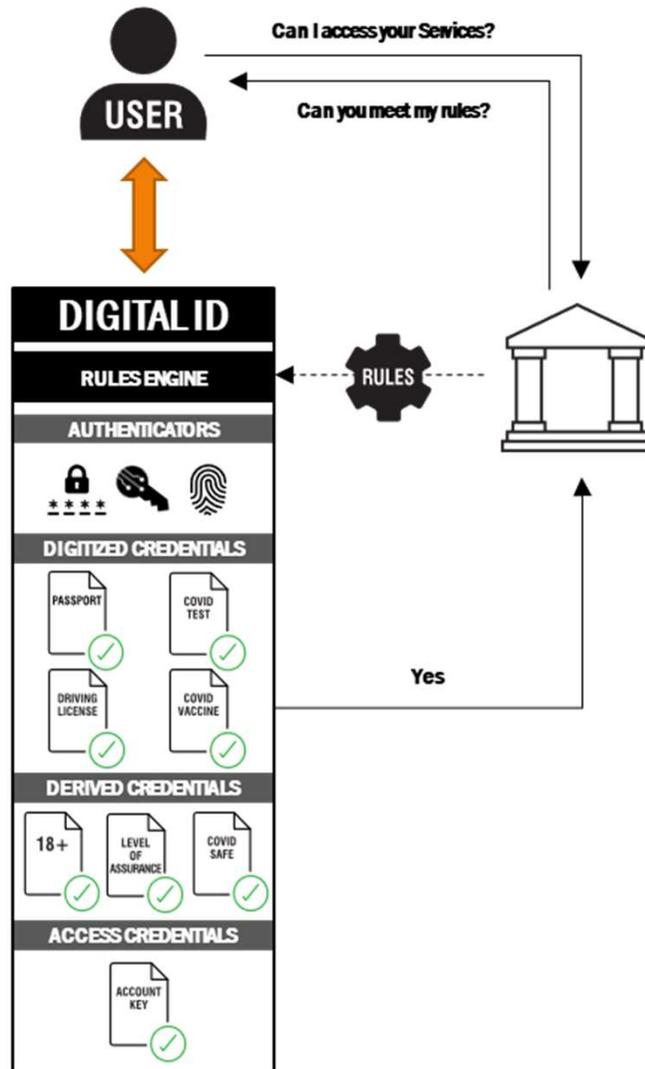


Making Digital ID a Success

OIX 2022  
Strategy  
Update

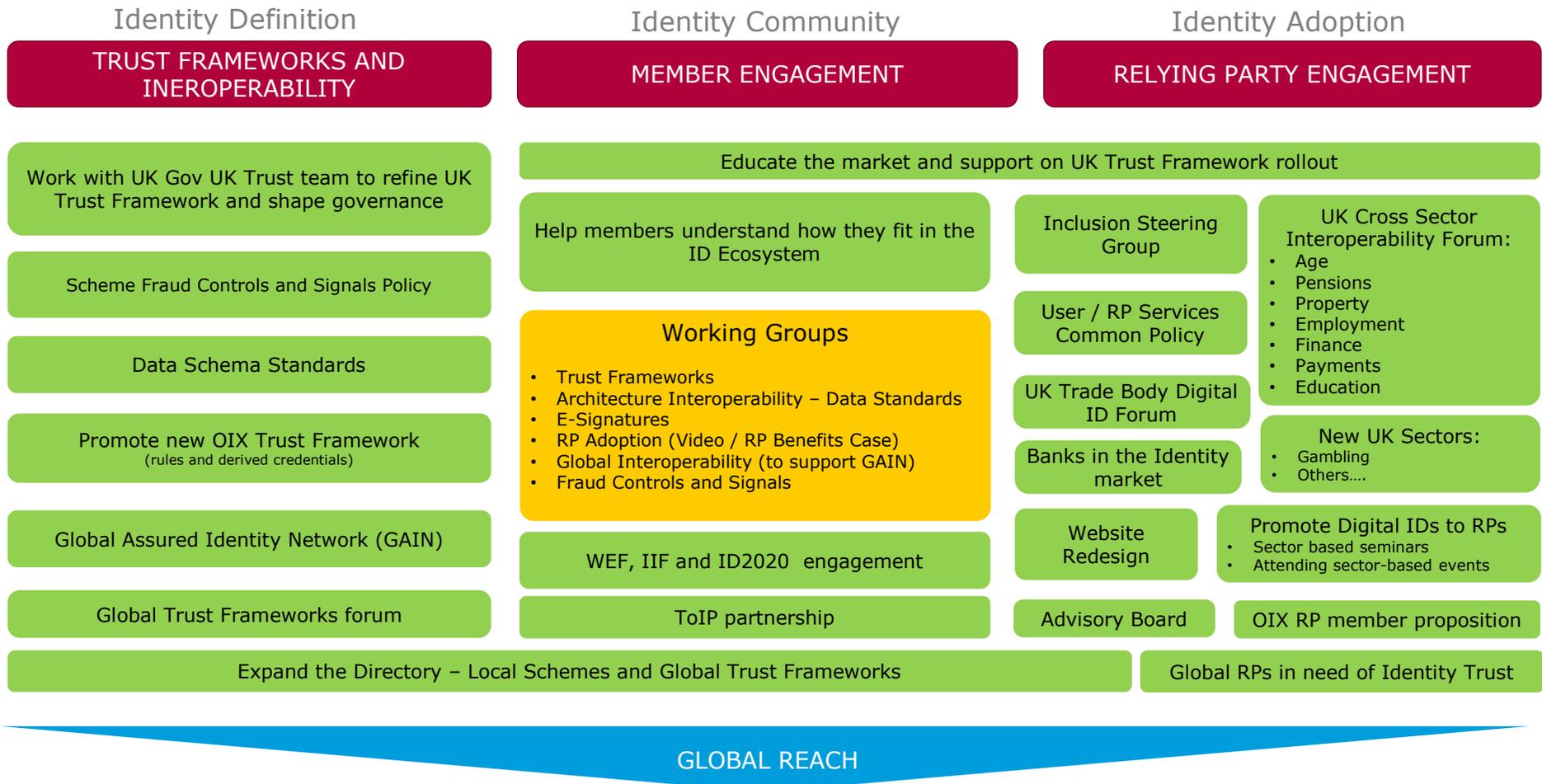


# OIX has launched its Trust Framework for Smart Digital ID



- Users can use a Digital ID to **confirm who they are**, and **share other important information about themselves**, to many different organizations who they want services from.
- The **Smart Digital ID works out what a user needs** to meet an organizations business rules **using a rules engine** or rules agent, and helps the user gather, derive and present credentials to meet the organizations needs.
- It can carry **digitized versions of existing credentials**, such a passport, driving license, vaccine certificate or relevant qualifications.
- It can also **derive credentials** that show users meet the business rules of an organization, **such as being over 18, COVID safe** or meeting a specific **“level of assurance”**.
- Organizations can also choose to allow users to use their **Digital ID to access an account** they hold with you. Thus, removing the need for you to issue your own logon authenticators (e.g., user IDs and passwords).

# OIX Strategic Plan 2022



RELYING PARTY REACH

GLOBAL REACH

Pan-global at a level above territories

# 2022 Working Groups



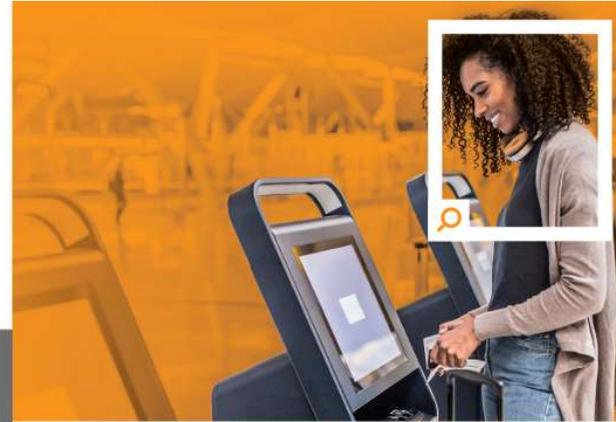
Working Group	Overview	Candidate Outputs
Trust Frameworks Evolution	<ul style="list-style-type: none"> <li>Overall overall OIX Trust Framework guide had been updated.</li> <li>Next steps will be to look at how OIX can provide more clarity on:               <ul style="list-style-type: none"> <li>Why an Intelligent Digital ID is required</li> <li>Clear confusion over decentralized / distributed/ centralized / federated.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>More on Smart Digital ID. Smart for the user?</li> <li>Clear the confusion over decentralized / distributed/ centralized / federated.</li> </ul>
Relying Party Engagement	<ul style="list-style-type: none"> <li>How can OIX further educate RPs on Digital ID and raise awareness of the business opportunity Digital ID represents? What are RP misconceptions of Digital ID and how can we remove those?</li> <li>What do end users see as the benefits of a RP allowing them to use a Digital ID?</li> <li>What sectors can OIX focus on to raise awareness? How to reach into these sectors (e.g. sector based projects / trade bodies).</li> <li>How can we get more RPs to OIX workshops and the Identity Trust Conference?</li> <li>Is there an RP OIX membership proposition? What value can OIX offer RPs?</li> </ul>	<ul style="list-style-type: none"> <li>Video</li> <li>New OIX Website area</li> <li>RP Proposition</li> <li>RP Benefits Case – commercial benefits.</li> <li>UK Market Sizing</li> <li>More RPs are the OIX conference in September.</li> </ul>
Architecture Interoperability	<ul style="list-style-type: none"> <li>There are 2 main protocols being discussed for DI: OIDC and DIDComm/VC. The evidence and claim data they carry is the same. Can a single core data schema work within each one? If a RP is dealing with multiple RPs that deliver data using different protocols, how can this be transformed into a single protocol in a secure and privacy preserving way?</li> </ul>	<ul style="list-style-type: none"> <li>Paper / Guide on Technical interoperability options and recommendations</li> <li>UK Cross Scheme Schema Standard.</li> </ul>
e-signatures	<ul style="list-style-type: none"> <li>How can a QES be qualified using a GPG45 standard Digital ID.</li> <li>Is there a mass market for Trust Services if the unit price for a QES is much cheaper, through more cost-effective ID proofing and authenticators.</li> </ul>	<ul style="list-style-type: none"> <li>TBD dependent on UK Trust Framework approach.</li> <li>Consumer market opportunity.</li> </ul>
Global Interoperability	<ul style="list-style-type: none"> <li>Looking a how to support GAIN, with other working groups / projects spinning out to look at detail.</li> <li>What areas of a trust framework are key for cross framework interoperability?</li> <li>How are key areas such as ID proofing standards assessed for interoperability?</li> <li>To avoid bilateral agreement explosion, how might a meta-framework – a <b>global interoperability framework</b> - be defined?</li> <li>How might cross framework interoperability be governed?</li> </ul>	<ul style="list-style-type: none"> <li>Key framework areas to assess to evaluate interoperability.</li> <li>Evolved Interoperability Assessment methodology.</li> <li>A Global Interoperability Framework.</li> <li>Governance model options and recommendations.</li> </ul>
Fraud Controls and Signals	<ul style="list-style-type: none"> <li>Work with UK Schemes to define the requirements for IdP fraud controls, information sharing and shared signals.</li> <li>What gaps does Digital ID introduce in existing RP fraud controls? What new fraud opportunities does Digital ID offer fraudsters? How might these be mitigated?</li> <li>What shared signals are required? How is a shared signal managed? What processes need to be in place when a signal triggers an alert? What happens when a party declares an ID fraudulent?</li> <li>How should signals be shared? Can this be done in a distributed way?</li> </ul>	<ul style="list-style-type: none"> <li>Fraud Controls and Signals Policy.</li> </ul>

Inclusion **Steering Group** is also continuing

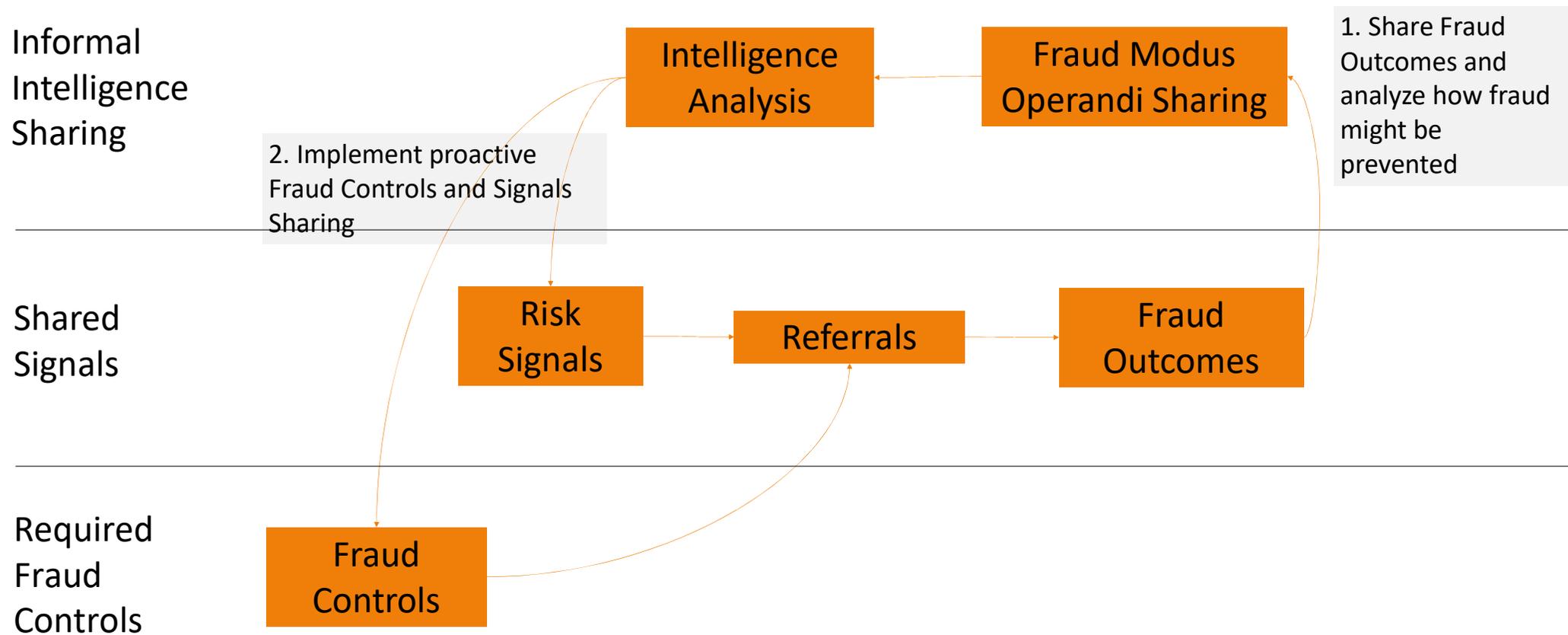


Making Digital ID a Success

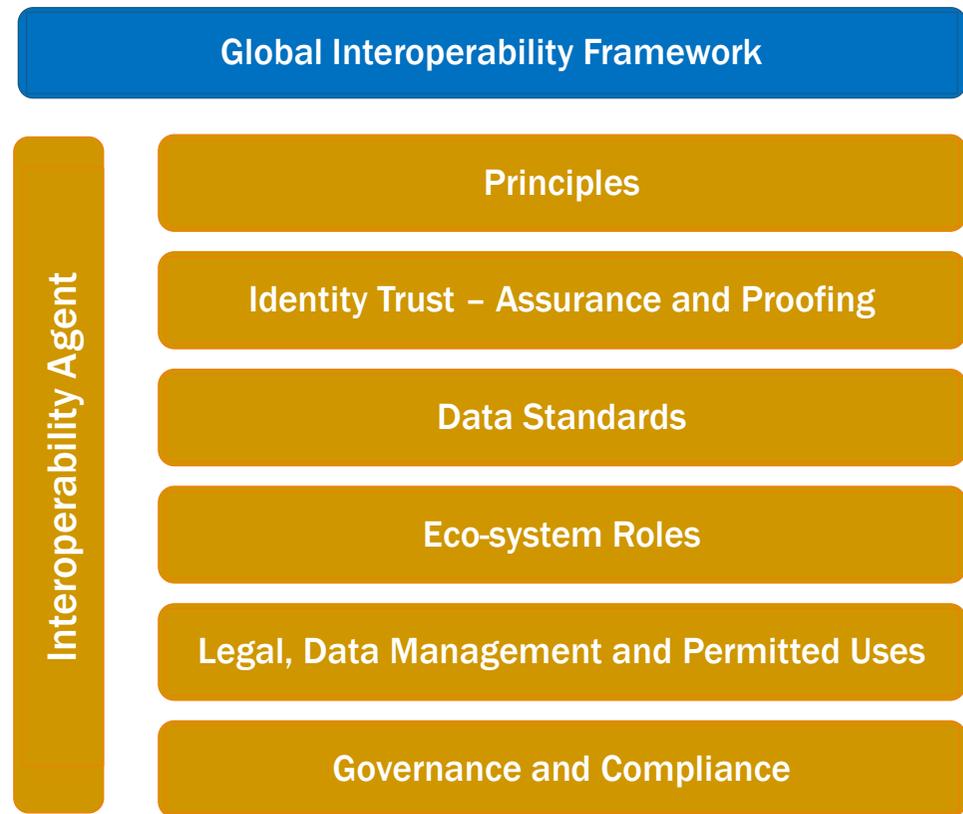
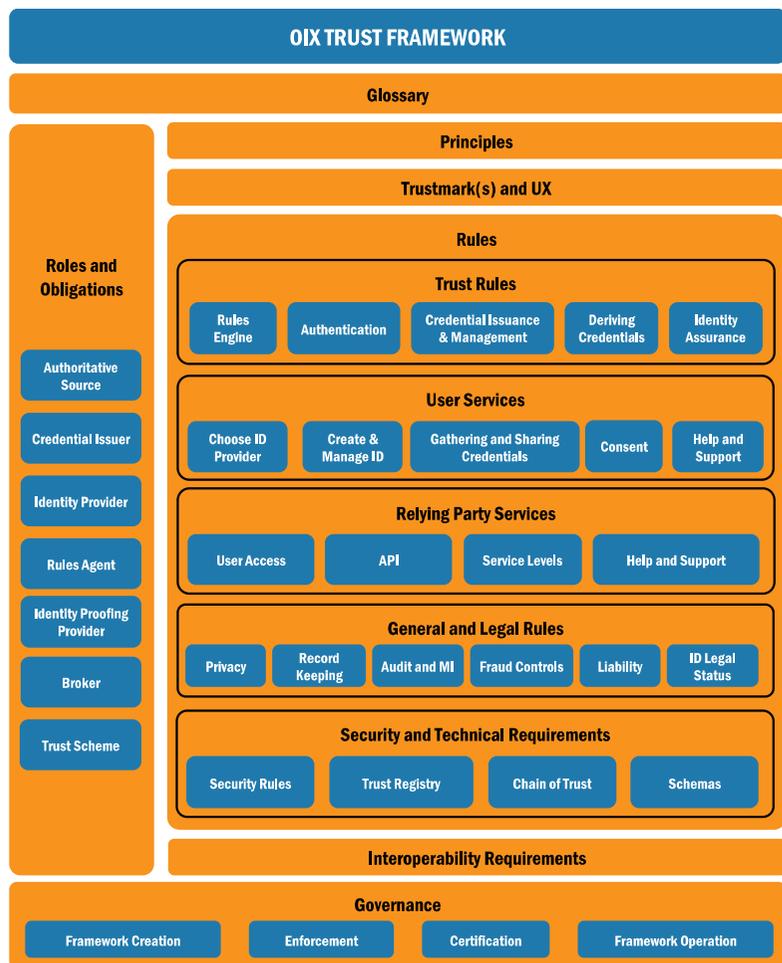
Working Group  
Highlights



# Fraud Controls and Signals - Implementation Approach



# Global Interoperability Framework



# Data Standards for “Core ID Information”



IN SCOPE

	Verified Claims	Assurance	Proofing	Evidence
<b>CORE ID INFORMATION</b>	Core ID Claims <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• DoB</li> <li>• Nationality</li> <li>• Contact Details</li> <li>• Personal Numbers</li> <li>• Image of Face</li> </ul>	Trust Framework Assurance Level Assurance Policy Assurance Procedure Assurance Elements and Scores: <ul style="list-style-type: none"> <li>• Strength / Validation</li> <li>• Activity</li> <li>• ID Fraud</li> <li>• Verification</li> </ul> Mapping Elements Scores back to Evidence	Validation Methods: <ul style="list-style-type: none"> <li>• Face to Face</li> <li>• Scanning</li> <li>• API Call using self declared data</li> </ul> Verification Methods: <ul style="list-style-type: none"> <li>• KBVs</li> <li>• OTCs</li> <li>• Selfie Cross Matches</li> <li>• Face to Face</li> </ul> Activity Methods <ul style="list-style-type: none"> <li>• Electronic Activity Evidence</li> <li>• Vouched Activity</li> </ul> ID Fraud Methods: <ul style="list-style-type: none"> <li>• Known Fraud</li> <li>• Risk Signal</li> </ul>	ID Documents <ul style="list-style-type: none"> <li>• Passport</li> <li>• National ID</li> <li>• Driving License</li> </ul> Electronic Records <ul style="list-style-type: none"> <li>• CRA Check</li> <li>• Bank Account</li> <li>• Electoral Roll</li> <li>• Fraud Check</li> <li>• Mortality</li> </ul> Vouches <ul style="list-style-type: none"> <li>• Via Digital ID</li> <li>• Face to Face</li> </ul>
<b>ELIGIBILITY</b>	Eligibility Claims <ul style="list-style-type: none"> <li>• Right to Work</li> <li>• Right to Rent</li> <li>• Driving Permissions</li> <li>• Travel VISA</li> <li>• Education Records</li> <li>• COVID Safe</li> <li>• Right to Vote</li> <li>• Bank Account Transactions (Open Banking)</li> </ul>	<ul style="list-style-type: none"> <li>•</li> </ul>		ID Documents <ul style="list-style-type: none"> <li>• Passport</li> <li>• National ID</li> <li>• Driving License</li> </ul> Electronic Records <ul style="list-style-type: none"> <li>• COVID Test</li> <li>• COVID Vaccine</li> <li>• CRA Check</li> <li>• Bank Account</li> <li>• Electoral Roll</li> <li>• Right to Work / Reside lists</li> </ul>

# Government Engagement

## United Kingdom

- Continue to provide feedback and pro-active suggestions on the UK Trust Framework
- Members have reviewed the latest consultation response
- 3 key areas for success:

Area	Approach for Success
Roles and end user "Positive Confirmation"	Existing B2B market must continue: regulated but uninterrupted
Legal Equivalence	Must include non-government ID based Digital IDs
Mobile Driving Licence	Must be delivered through the Trust Framework

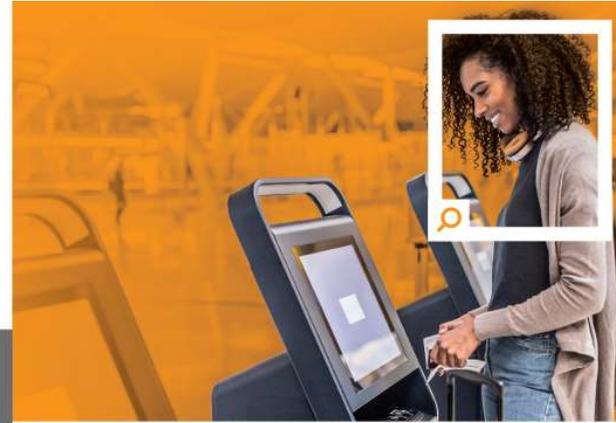
## eIDAS2

- Members have reviewed the Architecture and Requirements Framework (ARF)
- It is closely aligned with OIX's Trust Framework model. ✓
- It advocates for Smart Digital ID ✓ ✓
- There are a number of areas that could be clearer.
- OIXs response will be send to the eIDAS2 Expert Working Group.



# Making Digital ID a Success

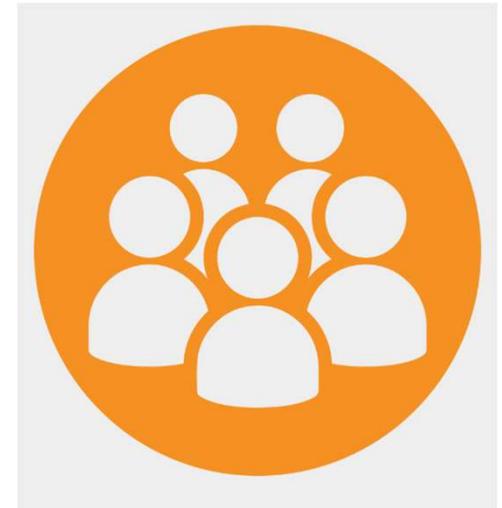
## OIX Membership



# Why join us?

## Member Benefits

- ✓ Take part in working groups and projects driving forward identity definition and adoption
  - Current working groups are looking at Trust Frameworks, Digital ID for Relying Parties, Architecture Interoperability, User and Relying Party Services and E-signature adoption
- ✓ Attendance at OIX member only workshops
  - We are currently running workshops with UK government on their new Trust Framework, as well as workshops with UK Banks
- ✓ Free access to all OIX papers and guides
- ✓ Product / Services listing on our online Directory
- ✓ Free attendance at our annual full day conference
- ✓ Input into key consultation responses by OIX
- ✓ Influence Stakeholders through the common voice of OIX
- ✓ Access to OIX member key contacts
- ✓ Networking opportunities
- ✓ Weekly news update
- ✓ Social Media engagement, collaboration & amplification
- ✓ Work with other members to define OIX strategy
- ✓ Opportunity to become an elected General Member representative on the OIX board
- ✓ Work collaboratively to drive adoption of digital identity by service providers





## Making Digital ID a Success

Wrap Up and  
Thank you!

