DRAFT EU-US TTC Digital Identity Mapping Exercise Report
OIX Feedback

February 2024 | Version 1.0

Produced by:
Nick Mothershaw with the input of the members of the
Open Identity Exchange Global Interoperability Working Group

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open License Terms

CONTENTS

This paper does not represent the views of the OIX member OFCOM.

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms

1 INTRODUCTION

In 2023 OIX analyzed 8 different trust frameworks, or schemes, from around the globe:

- EU eIDAS2
- US NIST Version 4 draft
- UK Digital Identity and Attributes Trust Framework (DIATF)
- Canada DIACC Pan Canadian Trust Framework
- Bank ID Sweden
- Thailand ETDA Trist Framework
- Singapore Singpass
- Modular Open-Source Identity Platform (MOSIP).

We divided our analysis into 2 areas:

- General Policy Rules for Digital ID for the 8 frameworks/schemes.
- Specific Rules and Approaches to Identity Assurance for 5 of the schemes that publish an identity assurance policy: EU, US, UK, Thailand and Canada.

OIX published its findings from this analysis and next steps in the report: Digital ID DNA – Interoperability Across Trust Frameworks

OIX thought it would be useful to share some of the learnings from this work in the context of the EU-US TTC digital Identity mapping exercise report as a response to the request for feedback that is in section 5 of that document.

We have separated our feedback into 2 areas:

- Identity Assurance – how levels of assurance can be calculated from evidence the user has associated with their Digital ID, which might manifest as credentials in a user's wallet.
- General Policy Areas – the similarities and differences we saw as part of our analysis, expressed using the characteristics and values identified as part of the OIX Open Criteria Exchange Tool (OCET), along with commentary about how these differences are salient when considering interoperability across the frameworks.

OIX's intent is to evolve and publish the Open Criteria Exchange Tool as a resource to allow frameworks to undertake comparisons when reasoning about interoperability. Ultimately OCET may be used as a way to publish policy in an open machine-readable form to allow other parties to consume, reason upon and adapt to a frameworks policy. We would wish to work with the teams and NIST and the EU to determine the requirements for a trust framework comparison and criteria exchange tool, along with other framework creators around the globe.

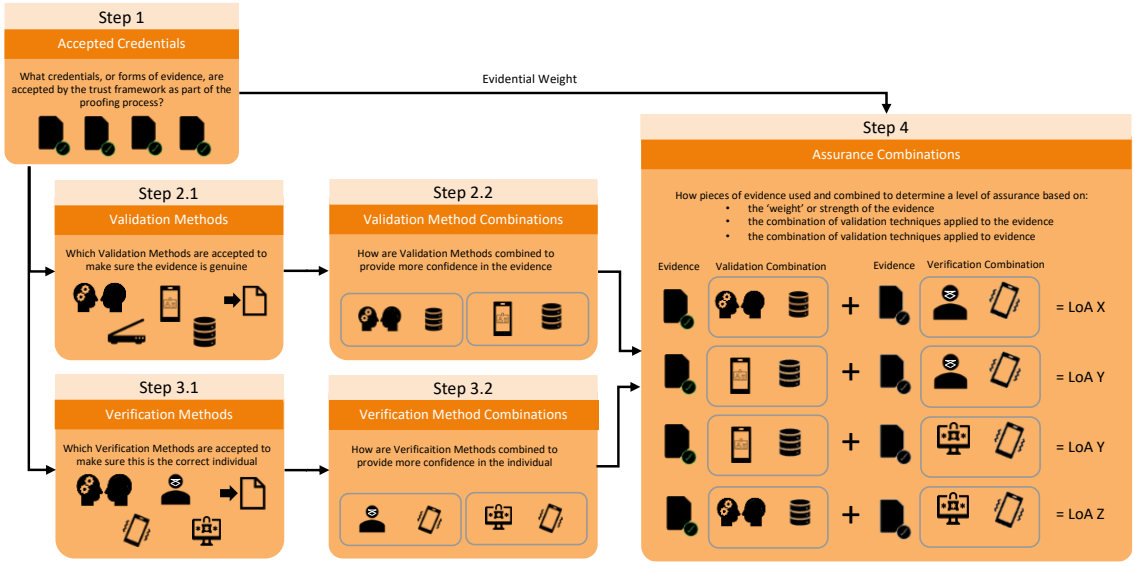
Please note that OIX's analysis was applied to the latest EU draft documentation for eIDAS2 in spring 2023 and the proposed NIST V4 documentation.

Our analysis team is not expert in either framework, nor the associated laws and regulations within which they operate. We may therefore have made some incorrect assessments or assumptions as part of our analysis and observations within this document. We aim to help show how the analysis we have done, and the Open Criteria Exchange Tool we plan to create, can be of help to the policy teams in the EU, US NIST and others around the globe.

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms

2 IDENTITY ASSURANCE POLICY

Through the analysis of the identity assurance policies of five of the frameworks we identified a common approach to proofing that can be applied when assessing credentials to determine a level of assurance:



This common approach to frameworks assurance policies – the **identity assurance policy model** - has the following steps:

Step No.	Step	Description
1	Accepted Credentials	Declare what credentials, or evidence is accepted as part of the proofing process. This could include specifying who acceptable issuers are, or the acceptable types of issuers.
2.1	Validation Methods	State which Validation Methods are accepted to make sure the evidence is genuine. Our analysis has identified five main validation methods that are used by frameworks: Validation of ID documents face to face (e.g., via an agent in a government office) Validation of ID documents using a specialist reader (e.g., scanner, NFC reader) Validation of ID documents using a smart phone (e.g., picture of document) Verification by accessing a database at an authoritative source (e.g., bank, credit reference agency, telco) ID credential can be directly validated back to the issuer (e.g., it is presented as a verifiable credential).
2.2	Validation Method Combinations	Explain how Validation Methods are combined to provide more confidence in the evidence. This combination step is the 'secret sauce' of identity assurance policies. Some frameworks combine the methods in different ways to increase the confidence, or score, obtained by the evidence in the identity assurance model. Not all frameworks do this, nor is it necessary for all levels of assurance in those that do.

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms

3.1	Verification Methods	State which Verification Methods are accepted to make sure this is the correct individual. Our analysis has identified five main validation methods that are used by frameworks: Verification of photo from ID documents to person face to face (e.g., via an agent in a government office) Verification of photo from ID documents against a separately captured image of the user (e.g., image taken by the user using their mobile phone) Logon to account that is in the user's control (e.g., logon to online banking or telco) One time code sent to a validated account (e.g., SMS to telco validated phone) ID credential can be directly verified back to the issuer (e.g., it is presented as a verifiable credential with the correctly bound authenticators).
3.2	Verification Method Combinations	Explain how Verification Methods are combined to provide more confidence in the evidence, in the same way Validation Methods are sometimes combined. Again, some frameworks combine the methods to increase the confidence, or score, obtained by the evidence in the identity assurance model. Frameworks tend to use combinations in the verification step less than in the validation step.
4	Assurance Combinations	How are pieces of evidence used and combined to determine a level of assurance based on: the 'weight' or strength of the evidence the (combination of) validation techniques applied to the evidence. the (combination of) validation techniques applied to evidence.

This maps to the steps highlighted in the EU-US analysis in the following way:

EU-US Process Step	**OIX Model Process Steps**
Evidence Requirements	1. Accepted Credentials
Validation Process	2.1 and 2.2 Validation Methods and Combinations
Verification Process	3.1 and 3.2 Verification Methods and Combinations
The sum of the Evidence Requirements, Validation and Verification Processes	4. Assurance Combinations

The EU-US analysis report highlights that there are similarities between the levels of assurance which makes them broadly align-able, but that there are also differences. The analysis at IAL2 / LoA2 starts with the comment that: 'Verification for both NIST IAL2 and EU LoA2 centers on the applicant's possession of identity evidence'.

This matches with OIX's key hypothesis: that levels of assurance can formulated from the evidence, or credentials, that a user holds in their wallet. LoAs can therefore can be formulated to meet the requirements of a destination trust framework as a wallet moves, or 'roams', from framework to framework. A NIST IAL2 can be formulated from the credentials a user holds in a EUDI Wallet, as can an EU LoA2 from credentials the user holds in a US based wallet.

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms

The identity assurance formulation process for each framework is different, with different values are assigned to different types of credentials, validations processes and verification processes.

So, if LoAs can be formulated from the trusted credentials held in a users wallet, alignment of LoAs across frameworks is not required, as formulation to a destination trust frameworks LoA is undertaken based on the credentials a user holds in their roaming wallet.

The table below shows some examples of how combinations of credentials can, or cannot, be used to formulate a NIST IAL2 and EU LoA2.

Evidence / Credential(s)	**How Validated**	**How Verified**	**EUDI Wallet, or it's agent, formulating NIST IAL2**	**US Wallet, or it's agent, formulating EU LoA2**
Digital Passport (in the future)	Issued directly by an authoritative source	Issued directly by an authoritative source that verified the user	Yes – assuming 5.2.7 address validation requirement is met because the EUDI wallet contain the users validated address.	Yes
Physical Passport	Chip crypto read	Selfie verification	Yes – assuming 5.2.7 address validation requirement is met because the EUDI wallet contain the users validated address.	Yes
Digital Driving License (mDL)	Issued directly by an authoritative source	Issued directly by an authoritative source that verified the user	Yes – a digital driving license is SUPERIOR evidence as it can be validated back to the issuer.	Yes
Physical Driving License with Chip	Chip crypto read	Selfie verification	Yes – as driving license with chip is SUPERIOR evidence. The crypto read of the chip validates it back to the issuer.	Yes
Driving License no chip	Scanned by third party	Selfie verification	No – as non-chip driving license is only STRONG evidence, so much be combined with other evidence	Yes

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms

Driving License no-chip + Bank Account	Driving license scanned by third party. Bank account validated as belonging to the person through bank verification service (e.g. 3DSecure*)	Selfie verification against Driving License image	Yes	Yes
Driving License no-chip + Bank Account	Driving license scanned by third party Bank account validated as belonging to the person through bank validation service (e.g. 3DSecure*)	Bank account ownership validated through bank verification service (e.g. 3DSecure*)	Yes	No – Photo ID not validated

*To use 3DSecure the wallet, or it's agent, must be a merchant and pay the associated fees.

As can be seen, the subtle differences in the two assurance methodologies result in different results for the same credentials.

For a user to achieve LoA2 in the EU and IAL2 in the US, they would need to have a wallet containing suitably trusted passport, driving license and possibly also bank account credentials.

In the EU national ID cards are a recognized form of evidence. US citizens will not have one of these so that does not help with interoperability in the US to EU direction. Recognition of national ID cards from other counties (e.g. the EU) in NIST would make interoperability easier for those who have and are willing to use a national ID card for verification purposes.

The introduction of open banking in the US would facilitate the validation of bank accounts in a consistent way.

To allow this LoA formulation process to happen, the credentials in the users wallet must be created and bound to the user using standards that each framework recognizes; the credentials must be trusted. This where there is a standards gap at the moment. Whilst standards are emerging for mobile driving license and digital travel credentials, these are not yet complete. Whilst there are many standards for bank accounts, there is no standard for bank accounts as a digital credential. As OIX progresses its work in this area, it will continue to raise the need for standards in these areas. In parallel, the OIDF Identity Assurance working group will be progressing the definition of schemas for these credential types.

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms

3 GENERAL POLICY RULES

One of the key findings of our analysis was that we found that trust frameworks around the world share common policy rule characteristics across 15 different areas covering roles, governance, legal, operational, and technical rules.

The 15 areas break down into 75 possible policy characteristics with 289 possible values.

Our analysis did not lead us to a conclusion that trust frameworks should or will normalize so that they have the same characteristics and values. Trust frameworks are necessarily different: they represent the same concept but within different legal, political, technical and ID ecosystem approaches. Whilst some normalization of characteristics and values may be possible as we see some very similar approaches across frameworks, we mainly see the results of our analysis as having identified legitimately different approaches within frameworks.

As a result, we expect the policy characteristics we identified will mainly be used to enable interoperability assessment and agreement between frameworks (and other parties), rather than alignment and normalization.

Our full analysis of the 8 frameworks is available to both US and EU policy teams, but is not contained in this document.

Using the OCET tool to analyse the US and EU frameworks there are three possible outcomes:

- the frameworks have policy criteria in common.
- one framework addresses criteria that the other does not.
- the frameworks address policy criteria in different ways.

Many policy criteria are already common between the EU and US, which is good news. The OCET tool enables these to be easily identified, and we have not focused on these in this document.

To aid understanding of the general policy area differences between the EU and US digital ID ecosystems, we are sharing below some of the key policy areas where, in our analysis, there are differences.

The draft EU-US report already covers an extensive analysis of roles and terminology, so we have not focused on those areas in this document.

Below we have highlighted the policy areas where one framework addresses criteria that the other does not, or where there are differences in criteria value settings for consideration when assessing interoperability between the 2 frameworks.

Policy Area	Criteria	NIST Values	EU Values	Observations
User Account Management	Account Closure Triggers	NIST covers the following account closure triggers where the user: -has not followed the terms of use they agreed to; -wants to close it; -account is inactive	EU requires account closure when the user dies.	There could be enhancements in both frameworks to adopt the values of the other. These differences are not a fundamental blocker when considering interoperability. However, the EU may have concern that the US based ID may be for a person that is deceased.

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms

Liability	Scheme and IdP liability	Is silent on matters of liability	Places liability obligations on the member state, and therefore their ID provider by proxy, for ID fraud and lack of availability.	This may pose a commercial challenge or the acceptance of US based IDs / Wallet Credentials in the EU.
Data Management	General	In the absence of federal legislation NIST are introducing in V4 data management requirements commensurate with EU GDPR	EU materials on ID are not that explicit in terms of data management, leaving this to GDPR.	The NIST enhancement to V4 for data management, or existing cyber security elements, may mean US wallets can be accepted in the EU.
Data Management	User Agreement for data sharing	Explicitly requires user agreement for data sharing	Leaves this to GDPR, which may lead some implementors to use implicit consent.	Wallets can adapt to this requirement when roaming to the other framework
Record Keeping	For RPs	No requirements for RP record keeping in NIST guidelines.	Records must be kept	Can an EU wallet be presented to an RP in the US without adding record keeping obligations? May need to assess other US regulations to which the RP is subject before understanding whether the US RP will meet EU requirements.
Record Keeping	Record of Proofing evidence retained	More detail on what must be kept: evidence used, authoritative sources used, authenticators bound	A general requirement for record keeping	If levels of assurance are to be formulated for the destination framework, the ID provider should keep the required evidence for that framework. So, if an EU wallet is used to formulate an US LoA, the evidence used should be recorded to US NIST guidance and vice versa.

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms

Risk and Incident Management	Data Breach	NIST is silent on this matter. Other US legislation may apply, in particular for financial services. Individual US states may have their own unique requirements.	User and RPs must be informed of data breaches. ID provider can be suspended as a result.	Do US wallets operating in the EU need to commit to these obligations?
Fraud Management	Types of Fraud Defended against	ID theft and synthetic ID	Does not specifically address fraud controls, other than liability in the event of ID fraud (see above)	Will EU wallets need to add fraud controls for the US? Or does the fact the liability for ID fraud lies with the EU member state mitigate this?
Fraud Management	Types of IdP Fraud Controls	US defines a list of control types that need to be considered: Basic ID risk indicators (dead, peps) Shared Risk Signals Device Risk Anomaly / Velocity Detection	Does not specifically address fraud controls, other than liability in the event of ID fraud (see above)	Will EU wallets need to add fraud controls for the US? Or does the fact the liability for ID fraud lies with the EU member state mitigate this?

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms

Fraud Management	Shared Signals	Specifies signals are required for: The account has been terminated. The account is suspected of being compromised. Attributes of the account, including identifiers other than the federated identifier (such as email address or certificate CN), have changed. The possible range of IAL, AAL, or FAL for the account has changed	No signal sharing specified	Will EU wallets need to add fraud controls for the US? Or does the fact the liability for ID fraud lies with the EU member state mitigate this?
Relying Party Requirements	RP Registration	No RP registration	Requires RP registration, with member state approval for use cases involving sensitive personal data.	Will EU wallets be able to used with unregistered US RPs? If it's not a US requirement for registration, this might be an area that can be lived with by the EU.
Technical and Security Policy	Security Policy Accepted	SOC2	ISO27001	Can these be accepted as equivalent in their effectiveness for the purposes of interoperability?
Technical and Security Policy	Cyber Security	Requires a policy to be in place, no standard referenced?	Requires: ENISA Cyber Security standards Regulation (EU) 2019/881	Can these be accepted as equivalent in their effectiveness for the purposes of interoperability?
Trust Registry	Who provides	Not part of NIST, left to implementors	Member States	Trust lists will need to be interoperable. Or wallets will need to be able to be added to and adapt to work within destination framework trust lists.

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms

Credential Standards	General	Is silent on the use of specific credential standards. It references OIDC and SAML as examples.	As part of the ARF specifies a number of specific standards for Storage, Encoding, Presentation, Selective Disclosure and messaging protocols.	Will US wallets need to adapt to EU presentation standards?

As can be seen from our observations, there is no single correct way to deal with the differences between the frameworks. The various approaches can be summarized as:

- Live with, or accept, the differences. Applying pragmatism to enable interoperability to be achieved.
- Add in policy elements that a wallet must meet before being accepted into the destination framework.
- Require wallets to dynamically adapt to meet the destination frameworks policy when 'roaming'.

Our analysis, and the proposed OCET tool, are intended to help frameworks agree interoperability approaches. We hope this analysis illustrates the need for such a tool to help frameworks achieve multilateral interoperability.

© Copyright | Open Identity Exchange | Licensed for use under the OIX Open Licence Terms