Digital ID DNA

Interoperability across Trust Frameworks

October 2023 | Version 1.1

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

CONTENTS

This paper does not represent the views of OFCOM.

Please note: The terminology in this paper is still being discussed within the OIX Global Interoperability Working Group and is subject to change.

1 EXECUTIVE SUMMARY

OIX's vision is that each of us can have a Digital ID that works seamlessly all over the globe. For this vision to become a reality, Digital IDs will need to interoperate across the regulatory and technical boundaries that are defined in trust frameworks, usually by a government or for a specific geographical area.

To advance this vision, OIX has been running a future looking working group looking at how global interoperability can be achieved. We have undertaken an analysis of the policies of 8 trust frameworks from around the globe to better understand their commonality and differences.

The good news is they do have a set of commonalities: 15 common general policy areas with 75 different characteristics and a common methodology to assess identity assurance. This is the DNA of Digital ID. However, like humans with DNA, the frameworks are not all the same. They have different values for the characteristics: 289 value variations across the 75 characteristics.

The results of our analysis will help frameworks understand their commonality and differences. It might allow them to align on some policy matters. But it is very unlikely that frameworks will align entirely as they are different for a reason. Diversity in policy at the detailed level is to be expected as frameworks are addressing the same policy issues in different ways to meet local variations in approaches to privacy, inclusion, risk, security, technology, and identity assurance. This diversity also means that undertaking many bilateral agreements between frameworks to achieve interoperability is likely to be an endless process; we need a more scalable approach.

We need to enable trust frameworks to interoperate, to communicate their value settings for specific characteristics as policy 'criteria' in a consistent way so that interoperability can be resolved, perhaps dynamically. To do this we have created the Open Criteria Exchange Tool (OCET) to allow policy criteria to be expressed and exchanged. OCET allows the communication of 15 areas of general policy rules and specific requirements for identity assurance as criteria: the values acceptable for a particular policy characteristic. OCET can be used in 'static' decision processes to explore policy criteria alignment and in 'dynamic' decision processes where policy criteria interoperability decisions are made 'on the fly'.

OCET will enable the creation of 'roaming wallets'; Smart Wallets that can operate in more than one framework through assessment of their conformance to the policy criteria of the destination framework they have roamed into.

Frameworks generally refer to one or more of 5 'golden credentials' in their identity assurance models: National IDs, Passports, Driving Licenses, Bank Account and Telco account. The proofing processing in their identity assurance models also leverage common methods such as document scanning and selfie cross match, but the detail on how these methods is executed are different within each framework. We have identified several areas of standardization that would enable better interoperability assessment, namely in the areas of credential formats and methods for validation and verification.

OCET enables parties to pose and answer the following four questions to achieve interoperability:

- Does a wallet have this right policy criteria to meet my requirements?
- Does a credential have the right policy criteria to meet my requirements?
- Can a wallet derive an attribute I need? (e.g., Over 18)
- Can a wallet derive a level of assurance I need?

Our creation of the OCET is still at an early stage, but we already see that it could offer enormous value in achieving interoperability of Digital ID on a global scale, enabling OIX's vision of allowing users to have a reusable Digital ID that works anywhere around the globe.

The OIX working group on global interoperability will continue. We will test the value of OCET with trust frameworks and other parties through desk top examination of the policy criteria requirements for some specific use cases.

Please join us on this exciting journey!

2 THE ANALYSIS AND APPROACH

The objective of analysis was to better understand the commonalities and differences between different implementations of Digital ID ecosystems around the globe to explore how interoperability of IDs across eco-systems can be achieved.

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

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

In selecting these framework and schemes, we deliberately wanted a mix of ecosystems that:

- Are mature and implemented a scale.
- Are evolving or new, and that are moving to embrace wallets.
- Represent the digital issuance of a government ID.
- Represent non-government provided ID under a government recognized trust framework, where federated private sector partners deliver Digital IDs.

Different countries have different strategies to deliver Digital ID. Some will deliver it centrally; some will federate it across private sector providers. We need to recognize that these models will co-exist when we consider interoperability. We cannot assume convergence of IDs to a common policy approach; government policies towards ID are inherently different around the globe and this is unlikely to change any time soon.

We divided our analysis into 2 areas:

- General Policy Rules for Digital ID
- Specific Rules and Approaches to Identity Assurance

The rational for this approach was that from our existing knowledge of trust frameworks we knew that Identity Assurance is sometimes a very detailed policy and process area in its own right, in particular where a country does not have, or want to have, a government issued foundational ID, for example in the US (NIST 800-63A) or the (UK GPG45). We wanted to understand if the processes and evidence used in these identity assurance policies was comparable. We also knew that most frameworks tackled similar general policy areas.

On analysis of the general policy rules for digital ID:

- We started off by directly analyzing the UK trust framework ourselves and grouping its policy into characteristics and values for those characteristics. We then validated our analysis with the DIATF team in the UK.
- We then analyzed the EU and US trust frameworks ourselves, drawing out more values for existing characteristics and new characteristics as we progressed. We then ratified our US analysis with the team at NIST.
- Having done the detailed policy analysis on 3 frameworks ourselves to make a start on the common policy characteristics, we created a questionnaire to allow frameworks to complete and extend the characteristics themselves.

- Questionnaires were then sent out and completed by the 5 remaining frameworks. The completed questionnaires were then collated into a central framework mapping, and the mappings we ratified with the contributing frameworks.

For the Identity Assurance Policy analysis:

- We again started off by directly analyzing the UK trust framework ourselves and categorizing the forms of evidence used, then the validation and verification techniques applied to that evidence to determine a level of confidence in the ID.
- We then analyzed the EU and US trust frameworks. This showed that they used common evidence types with the UK trust framework, and also common validation and verification techniques. However, the important thing we identified is that this evidence and associated validation/verification technique were combined differently to meet local levels of assurance in line with local policy and risk appetite. So, essentially the same methodology, but different combinations and scores.

We realized at this point that it would be difficult to hand this part of the analysis over to the frameworks themselves as our objective became to map each frameworks policies into the methodology we have identified, to prove whether this methodology worked for more frameworks. We continued to analyze evidence-based identity assurance polices ourselves where they exist and did so for Canada and Thailand.

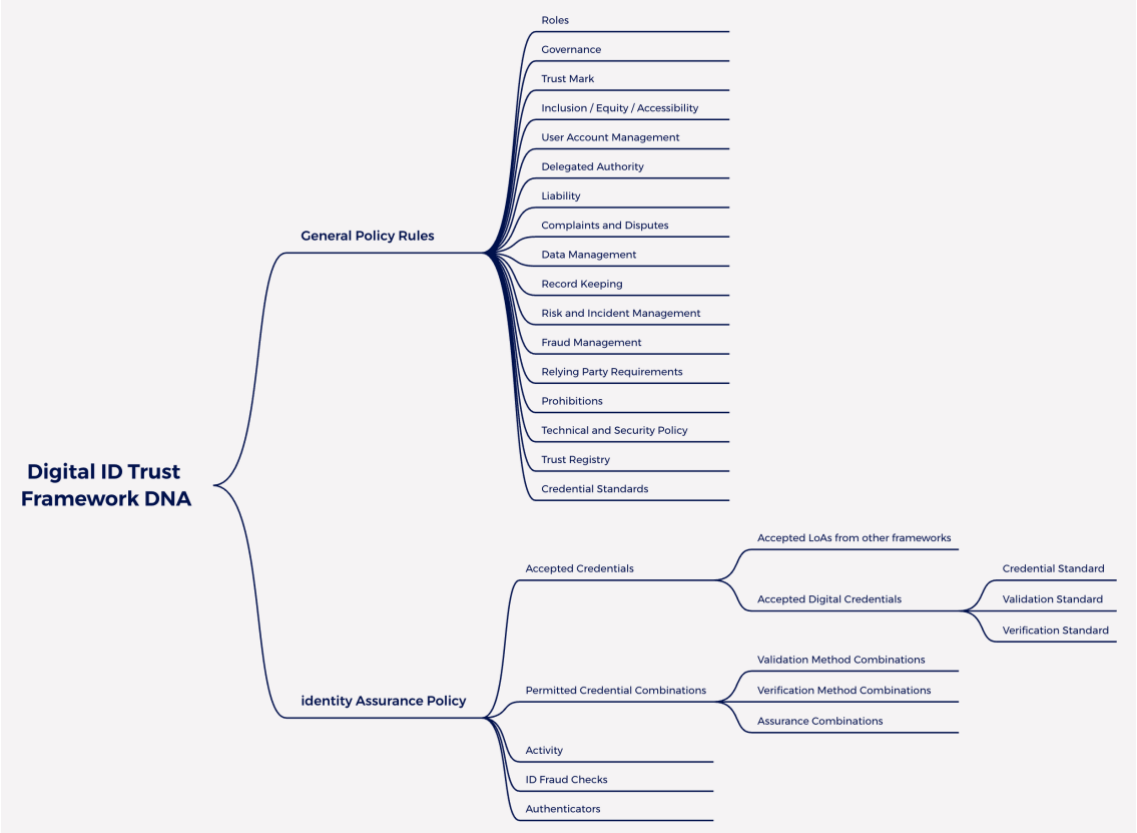
Not all the frameworks have a complex Identity Assurance policy that uses different evidence types for us to analyse. This is the case for:

- Singapore – where a government issued ID is used to create a digital Singpass.
- Bank ID Sweden – where face to face checks to an AML regulatory standard in a bank branch are used to issue an ID.
- MOSIP – where the approach to ID proofing the user into the ecosystem is a local policy matter.

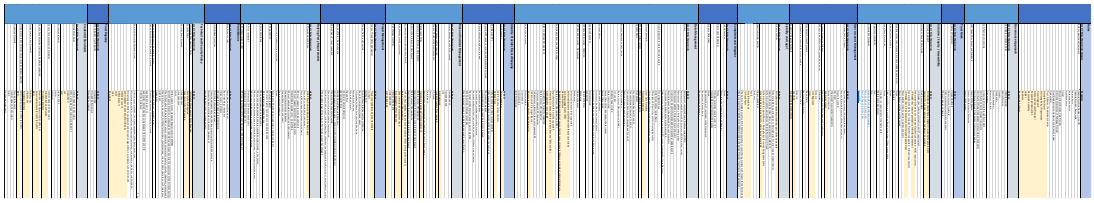
MOSIP completed for a typical customer, MOSIP itself a trust framework implementation but a solution template to deliver national ID eco-systems. One of the big challenges is building implementations that are inclusive for all systems, so exceptions to policy may be required in order to achieve this.

3 FINDINGS – THE DNA OF DIGITAL ID

Our key finding was that we found that trust frameworks around the world work to a common Digital Identity DNA. They share common policy rule characteristics and a common approach to identity assurance policy:



We called this the Digital Identity DNA because of how the analysis looks when it's laid out and observed from a high level:



It reminded our researchers of a DNA sequencing diagram. We also think it serves as a good analogy: humans are the same species, but our different characteristics are what make us unique, and the same goes for trust frameworks.

We have grouped the analysis into two areas:

- General Policy Rules. Split into 15 policy areas covering roles, governance, legal, operational, and technical rules.
- Identity Assurance Policy: the specific rules around establishing trust in the user (proofing) and ensuring the genuine user then presents the ID (authenticators).

These two areas are expanded upon in more detail in sub-sections below.

Our analysis does 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 these policy characteristics will mainly be used to enable interoperability assessment and agreement between frameworks (and other parties), rather than alignment and normalization.

3.1 General Policy Areas

Each Policy Area contains one or more Policy Characteristics that a framework might address. Each Policy Characteristic has its own set of possible Values.

In terms of general policy areas, our analysis identified 15 common general policy areas, containing 75 policy characteristics with 289 possible values.

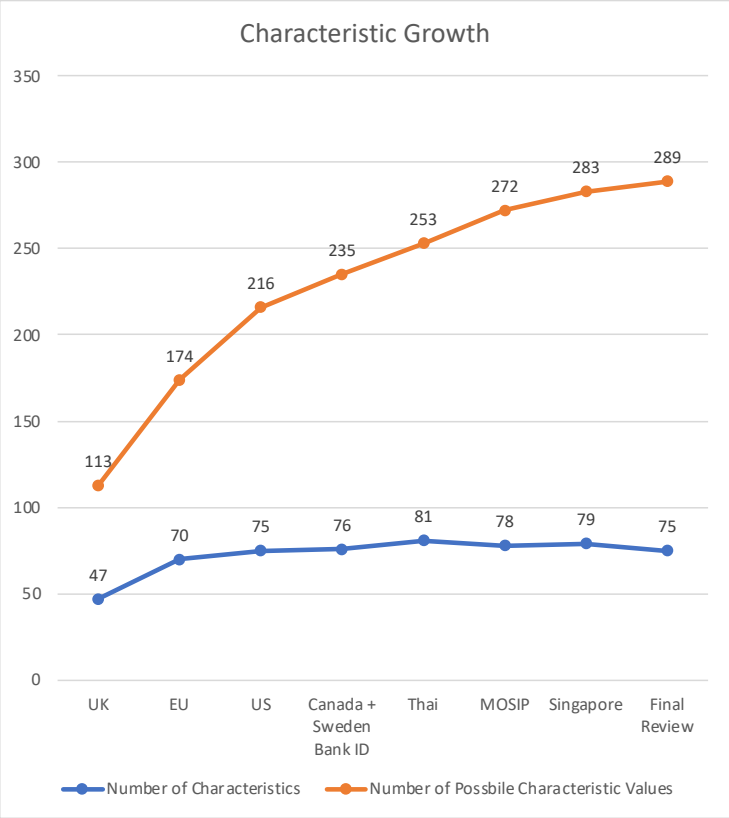
The 15 policy areas we have identified are:

Policy Area	No. of Characteristics	No. of Possible Characteristic Values	Characteristics addressed
Roles	1	20	Which roles does the framework recognize? For example, relying parties, identity providers, issuers.
Governance Approach	3	14	Does the framework formally certify or license participants? If so which ones?
Trustmark	1	4	Does the framework issue a trust mark? Who must display it?
Inclusion / Equity / Accessibility	7	23	Must parties have an inclusion policy or plan? How is inclusion monitored? What accessibility standards must be met?
User Account Management	6	18	What triggers account closure or suspension? Who must close / suspect accounts? How is fraud handled? Is delegated authority supported?
Liability	2	13	Who is liable for error or fraud, and in what circumstances?
Complaints and Disputes	3	9	Is there a process? Who takes responsibility?
Data Management	13	55	What is the Data protection and privacy policy approach? Including: Consent, Data minimization, Tell us once, Right to be forgotten, Portability
Record Keeping	4	13	How long must records be kept for? By whom?
Risk and Incident Management	9	21	What standardized processes must be followed? How are data breaches handled?
Fraud Management	4	17	How must parties look for fraud and how to they collaborate to address and reduce fraud?

Relying Party Requirements	6	22	What are the obligations and restrictions on relaying parties when using Digital IDs.
Prohibitions	2	8	What are parties not allowed to do?
Technical and Security Policy	6	26	What standardized processes must be followed? What encryption approach and methods are required?
Trust Registry	1	3	Does the framework provide a list of parties who are part of the framework? Is this machine readable?
Credential Standards	7	23	What standards are accepted for issuance, storage and presentation of credentials?

These policy areas align well with policy headings for frameworks suggested in the OIX model trust framework.

As we progressed through the analysis from framework-to-framework we have tracked the rate of growth of the characteristics and their possible values. If this was growing linearly with each new framework analyzed that would mean there is no commonality across the frameworks, which would be bad news for the chances of achieving interoperability. The good news is that the rate of growth slowed as we analyzed more frameworks:



As we went, we undertook some merges of obviously duplicate characteristics and values, which is why the number of characteristics drops from time to time.

This slowing of growth indicates that we are finding the common characteristics and values used across the set of frameworks and that the number of possible characteristics and values is probably finite. The growth curve is expected to continue to level as we complete more analysis.

The following example shows the policy characteristics and possible values in the area of Data Management, which is the largest policy area in terms of possible values:

Data Management	
Level 1 Policy Characteristic	**Values1**
Privacy	Parties must complete Privacy Risk Assessment/DPIA
	Parties must publish Privacy Risk Assessment/DPIA to other p
	Parties pust publish a Privacy Policy to other parties
	Parties pust publish a Privacy Policy to end users
	Users must be sent information about ID proofing / update ev
	Explicit consent must be gathered for use of biometrics
	User consent to privacy policy must be recorded
	IdPs must use technical measures to ensure RPs cannot work
User Agreement for Data sharing required	For all lawful basis
	Only for consent as lawful basis
	Through an Alllow List as of static trust agreements
	Through Explicit Consent In dynamic trust agreements
Consent Approach	Local Data Protection
Who must collect consent	Most apprpriate party
Consent Basis	No Consent
	Consent through general Ts and Cs
	Consent through allow list in Ts and Cs
	Consent through explicitely acknowledged Ts and Cs
	Explicit consent for each transaction
Consent Approach to Data Listing	Does not address
	Refers to local DPA legilsation (GDPR)
	In Ts and Cs
	Evidence Types Listed
	Data Items Listed
	Actual Data Listed - Masked with user reveal
	Actual Data Listed
Consent history	No explicit reference
	Users must be able to see consent history
	Users must be able to see consent history with list of data sh
Long Lived Consent	Not referenced
	Supported
IdP Data Minimisation - Collection	Does not Address
	Mandatory
IdP Data Minimisation - Presentation	Does not Address
	Mandatory
	Selective Disclosure to be supported
	Zero Knowledge Proofs (ZKP)
	Derived Predicate
	Requesting Organization must ensure that the consent reques
Porting data from one IDP to another	Refers to local DPA legilsation (GDPR)
	Explicitely states this must be supported
	Generally, it is not possible to port data from one IdP to anoth
	Not Applicable - only one IdP
Right to be forgotten approach	No right to be forgotten supported
	Refers to local DPA legilsation
	User must approach RP themselves
	IdP generates a letter for the user to approach RP
	IdP instructs RP to forget the user
	RP must remove data for closed Digital ID
Tell us one approach	Not supported
	User consent
	User selection
	All RPs informed

Other policy areas are much simpler, such as the Risk and Incident Management area:

Risk and Incident Management	
Level 1 Policy Characteristic	**Values1**
Quality Management Policy Accepted	ISO 9001:2015
	ISO 20000:2018
	ITIL
	Not Addressed
Indicent Response Plan required	Incident Response Plan required
Types of Incident IdP must respond to	ID Fraud
	Service
	Data Breach
	Disclosure to law enforcement on legitiate request in home r
Data Breach Policy	Framework requires policy for data breach
User must be informed of Data Breach	Refers to local DPA legilsation
	Explicitely states the User must be informed of Data Breach
RP must be informed of Data Breach	Refers to local DPA legilsation
	Explicitely states the User must be informed of Data Breach
Suspension of service due to data breach	IdP can be suspended in the event of a data breach that affec
	Refers to local DPA legilsation
Risk Management Plan	Risk Management Plan Required
Supported Risk Standards	ISO/IEC 27005:2018
	ISO31000:2018

In this example we see that some characteristics have values that point to the requirement for complex standards to be in place, such as ISO9001:2015.

In some areas we can we that a policy characteristic is overloaded: the spread of values are actually describing different sub-characteristics. In these instances, we need to the overloaded characteristics into to 2 clearer characteristics.

The full list of 75 characteristics and their 289 values is not being published at this stage of the programme. The intent is to work with the participating frameworks to normalize the characteristics where possible and then to ultimately publish them as an open framework.

The table below summarizes first impressions that we have gathered. The initial analysis has fulfilled our goal of investigating and understanding which characteristics and values could be defined by a subset of trust frameworks. This has provided a foundation for future work to further understand potential prioritization of characteristics and values by trust frameworks among other aspects.

However, we can share a summary of our findings for each policy area:

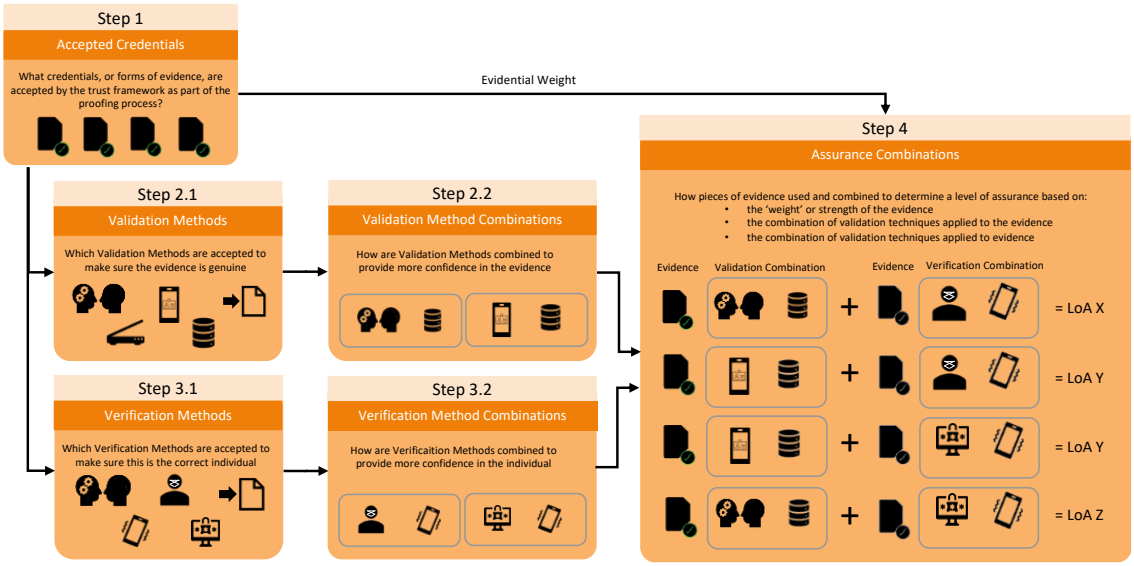
Policy Area	Summary of Findings
Roles	All frameworks cover the roles of relying party and re-usable ID provider. 5 of 8 support Trust Schemes/Federation Schemes, Orchestrator and Authoritative Source roles
Governance Approach	Of the frameworks (7/8 frameworks) that stated certifiable items/roles, 71% formally certify ID Providers (5/7 frameworks).
Trustmark	75% of frameworks issue a Trustmark, but only 50% require ID Providers to display this to end users.
Inclusion / Equity / Accessibility	All frameworks require accessibility provisions. Only half the frameworks currently have an inclusion strategy, but this is an area all are seeking to address going forward.
User Account Management	Circumstances in which an account needs to be closed varies greatly across the frameworks. 5 out of 8 frameworks address recovery of fraudulently used IDs.
Liability	Half the frameworks afford Digital ID the same legal status as a physical ID. Also, only half the frameworks enforce some form of fault-based liability on ID Providers in the event of fraud.
Complaints and Disputes	75% (6 out of 8) of frameworks have a complaints and disputes process

Data Management	Is the most complex area addressed by frameworks, implying that this area has the most types of characteristics and respective values. 100% of frameworks require that Parties must publish a Privacy Policy to end users. 7 out of 8 require data minimization to be applied on credential presentation and require some form of consent history to be made available to the user. 3 of 7 frameworks that answered support 'tell us once'. There are 6 different approaches to data listing as point of consent to share; only 2 frameworks share a common approach.
Record Keeping	100% of frameworks have a record keeping requirement.
Risk and Incident Management	Half the frameworks leverage ISO standards to meet this requirement.
Fraud Management	25% (2 of 8) of frameworks do not address fraud management. Of the 75% that do, 50% only have generic statements that fraud must be monitored, whereas the other 50% require detailed types of fraud controls. 5 of 8 frameworks share data across parties to ensure fraud is detected and managed.
Relying Party Requirements	Half the frameworks have no specific obligations that are aimed at relying parties.
Prohibitions	The most common prohibition is that ID Providers must not do anything illegal. Of the 6 frameworks that address ID prohibited data uses, 5 of them prohibit any form of processing without the user's agreement.
Technical and Security Policy	7 of 8 frameworks reference ISO27001 as a preferred or required security standard.
Trust Registry	3 of 8 frameworks provide a trust registry themselves. 3 of 8 require schemes to provide a trust registry. 3 of 8 do not provide a trust registry
Credential Standards	Some frameworks reference credential standards as supported examples, whilst others prescribe the use of specific standards. The range of referenced credential and protocol types is significant with 6 characteristics having 23 possible values.

Next Step: Work with participating trust frameworks to see if any normalization/sub-division of characteristics and values is possible and identify which are most important when considering interoperability. Do this as part of use case-based policy applicability analysis.

3.2 Identity Assurance Policy

Through the analysis of the identity assurance policies of five of the frameworks we have 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.

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.

An example of some assurance combinations from the Thai trust framework would be:

	Validation					Verification				
	Credential A		Credential B			Credential A		Credential B		
Assurance Combination	Credential	Validation Combination	Credential	Validation Combination Code		Credential	Verification Combination	Credential	Verification Combination Code	Level of Assurance
Passport + Telco	Passport	NFC Chip Read	Telco Account	Validated against Authoritative Source		Passport	Verification of photo from ID documents against a separately captured image of the user			IAL2.1
Passport + Telco	Passport	NFC Chip Read + Validated against Authoritative Source	Telco Account	Validated against Authoritative Source		Passport	Verification of photo from ID documents against a separately captured image of the user	Telco Account	One time code	IAL2.2

In this example we see that credential A has a validation combination of 'NFC Chip Read PLUS Validated against Authoritative Source' when being used to achieve IAL2.2

This same methodology can be applied where a government ID is issued by an agent, but in a simplified execution format i.e.:

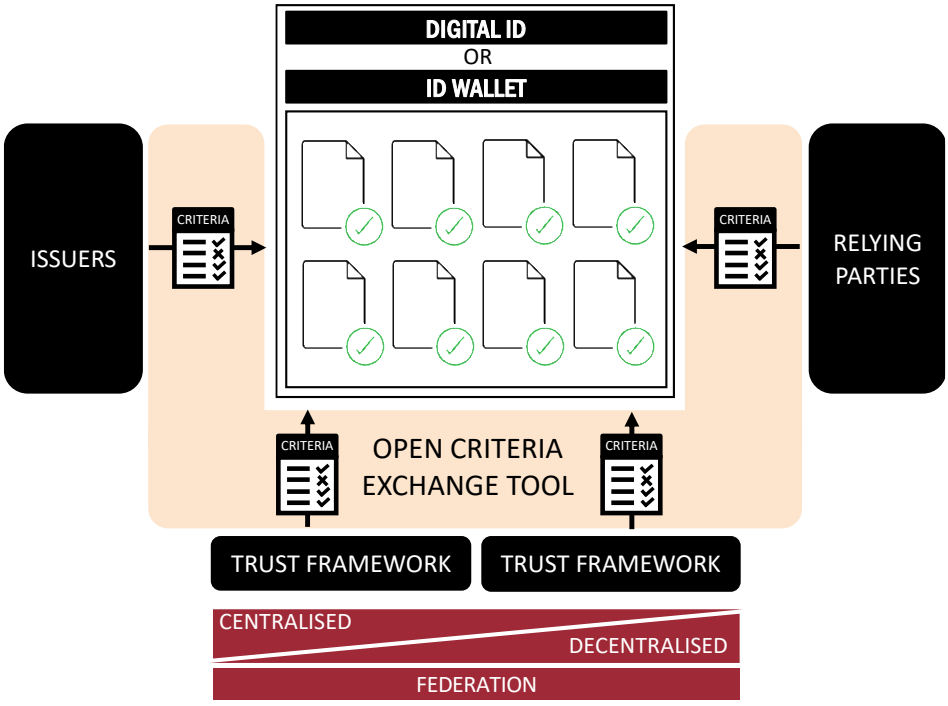
- Accepted Credential: Physical Government ID
- Validation Method: Validation of ID documents face to face (e.g., via an agent in a government office)
- Verification Method: Verification of photo from ID documents to person face to face (e.g., via an agent in a government office)
- Level of Assurance Combination: Physical Government ID: Validated face-to-face and Verified face-to-face = LoA X

4 OPEN CRITERIA EXCHANGE TOOL

The Digital ID DNA we have discovered can be used to create a tool to allow parties to communicate their policy requirements, or criteria. We have named that tool the Open Criteria Exchange Tool – OCET. This tool comprises:

- The 15 General Policy Rule areas the analysis has identified.
    - Within these areas, the list of policy characteristics (75) and possible characteristic values (289). This is expected to continue to grow as more parties leverage the framework.
- The Identity Assurance Policy Model, comprising:
    - Required Claims
    - Accepted Credentials
    - Accepted Validation Methods and permitted combinations.
    - Accepted Verification Methods and permitted combinations.
    - Level of Assurance matrix approach
    - Authenticators

Parties can communicate value settings for specific characteristics as **criteria** using OCET:



Party	What is being communicated
Trust Framework	Trust Framework criteria
Credential Issuer	Credential use criteria
Wallet	Supported criteria, based on trust framework certification and commercial position
Relying Party	Acceptable criteria to meet their use case and regulatory obligations

OCET is an open tool that each party can use to publish their policy criteria in a way that other parties (who they trust) can read. It does not require any central infrastructure to enable this; each party expresses and publishes their own criteria using OCET characteristic and value combinations. These are classic 'key-value' pairs, which means other parties read this from to make policy decisions.

The following table contains some examples of criteria definitions using OCET:

	CRITERIA	
General Policy Area	Policy Characteristic	Acceptable Value(s)
Governance	Certification or Licensing	ID Providers must be certified directly through framework
Trust Mark	Display of Trustmark	ID Providers must display Trustmark to end users
Inclusion / Equity / Accessibility	Accessibility Guidelines	WCAG
User Account Management -	Account Closure Triggers	has not followed the terms of use they agreed to. wants to close it. has died. account was created fraudulently
Data Management	Consent Approach to Data Listing	Actual Data Listed
RP requirements	RP flow down conditions	Prohibited processing rules - no profiling.
Technical and Security Policy	Security Policy Accepted	ISO27001
Accepted Credentials	Credential Type	Driving License, Passport, National ID
Accepted Credentials	Credential Format	mDL, DTC
Accepted Credentials	Issuer Type	Government Agent
Verification	Verification Method Combination	Selfie Biometric

OCET is entirely technology and ID paradigm neutral. It can support any implementation of Digital ID:

- Those issued by governments or those issued by the private sector.
- Those leveraging a 'centralised' or 'decentralised' architecture.
- Where a federation of ID providers is operated.

4.1 How can OCET be used?

The OCET can be used in the following scenarios:

- **For framework creation and evolution.** Those who are creating a new trust framework for Digital ID or those that already have a framework that is being evolved or extended can use the OCET as a reference point for how other frameworks are addressing policy criteria. Choosing to use existing policy characteristic and values from OCET when defining policies will make interoperability with other frameworks easier.
- **In framework-to-framework discussions on bilateral agreements for interoperability.** The OCET can be used as a start point for frameworks to self-analyze their relative policy criteria positions. With this information documented in a common language the frameworks can then easily see commonalities and differences, and agree whether differences can be lived with, or whether step-up processes are required to achieve interoperability.
- **In a static definition of what policy criteria are acceptable**. A trust framework or relying party might use the OCET to determines which wallets and credentials, from which other frameworks, are acceptable to them. These might then be placed on a trust list of acceptable wallets and credentials. For example, the UK might use the OCET to analyze the Pan Canadian Trust Framework (PCTF) and as a result state that wallets from the PCTF that meet specific criteria are acceptable in the UK, with a filtered list of what the accepted credentials from those wallets might be.
- **In a dynamic transaction-based interaction.** Here a relying party might use the OCET to express its policy criteria to a wallet. The relying party might lean on the policy criteria of its prevailing trust framework when it does this (e.g., I want this LoA from my trust framework). The wallet can then dynamically determine whether it can meet those policy requirements, based on the policies it supports and the policies of the credentials it is holding.

So, OCET can be used to agree bilateral and multilateral interoperability agreements, but this is not scalable.

However, to achieve scale, **dynamic transaction-based** interactions will be the way forward, where Smart Wallets that transcend framework boundaries read and dynamically adapt to expressions of policy criteria from all parties.

For dynamic transactions, a machine-readable form of the OCET policy criteria expressions will be required.

Next Step: Explore what a machine-readable format of OCET might look like. Consider which existing technical specifications could be extended to communicate this format.

5 IDENTITY ASSURANCE AND INTEROPERABILITY

When making interoperability assessments regarding a level of assurance we have identified two approaches that frameworks may use to determine if it's identity assurance requirements can be met:

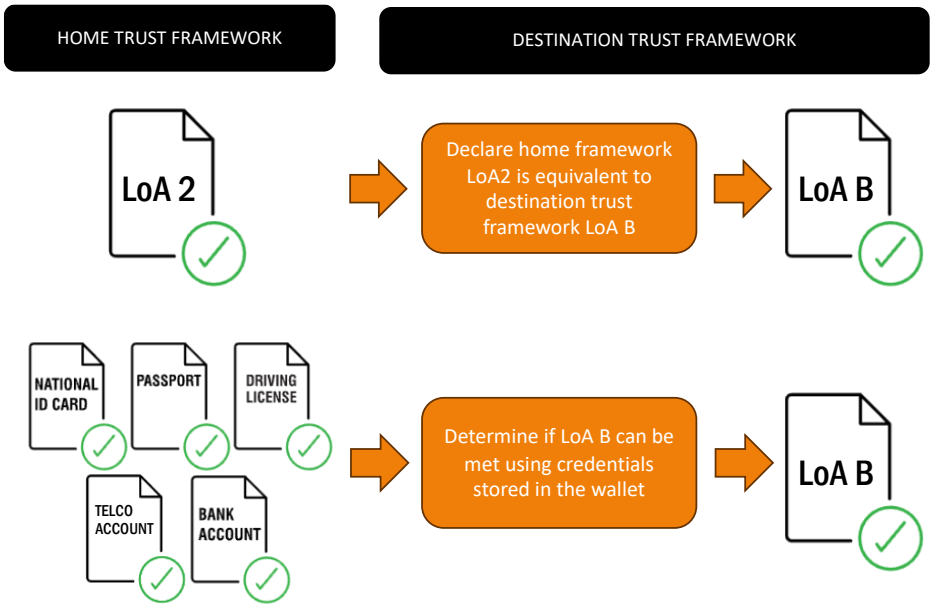
1. Accept a level of assurance from another framework, for example a level of assurance might be declared equivalent to one in the destination framework (e.g., EU declared that NIST IAL2 is equivalent to EU Substantial).

This first option is likely to be leveraged on a bi-lateral basis when agreeing digital ID interoperability between cooperating frameworks. However, due to the complexity of manual assessment required that option is unlikely to scale.

2. Use credentials that were issued under a wallets **home trust framework** to determine whether local framework policy criteria for Identity Assurance can be met in a **destination trust framework**. For example, do the passport and a bank account credentials allow the achievement of a level of assurance in the destination framework.

This second option can be done dynamically when a wallet encounters the new destination framework, enabling interoperability to scale. However, it requires the destination framework to be able to accept and trust the credentials in the wallet.

The diagram below illustrates these two different options:



OCET supports both these scenarios.

Option 2 requires standardization of not only of the credentials used, but also how they are proofed into the wallet.

6 IDENTITY ASSURANCE STANDARDS REQUIRED

To allow the determination of a level of assurance in a destination trust framework using credentials issued under a wallets home trust framework, standards will be required for credentials in respect of:

- The required claims
- Their format
- How they are proofed
- Authenticators required to assert them.

The need for data standards for required claims is explored in the recent OIX paper Data Standards for Digital ID Interoperability.

The type(s) of authenticator that may be bound to a credential and used to present identity assurance is addressed in many of the trust frameworks we have analyzed. However, our analysis of trust frameworks to date has not considered in detail standardization for authenticators in the context of identity assurance. This could be a next step for the OIX working group to consider as it evolves the OCET.

Next Step: Further analysis on authenticator standards referenced by trust frameworks and consideration of standards required (existing and new) to enable interoperability.

6.1 Credential Format – 5 'Golden Credentials'

As part of our analysis of identity assurance policies we discovered that frameworks tend to leverage the same core credentials as part of the ID Proofing process to attain a level of assurance:

Credential	Framework A	Framework B	Framework C	Framework D	Framework E	Digital Credential Standard
National ID Card		Y		Y	Y	
Passport	Y	Y	Y	Y	Y	DTC
Driving License	Y	Y	Y	Y	Y	mDL
Bank Account	Y		Y		Y	
Telco Account	Y		Y		Y	

These 5 **'golden credentials'** are common to many countries and are the ways that a user's physical identity can be validated and verified.

It is worth noting that where frameworks refer to a national ID card or driving license it is often a reference to the locally issued document, not a reference to an interoperable form of credential from another framework domain. For Passports, Bank Accounts and Telco Accounts the reference is less likely to be constrained to those that are issued locally to the domain of the trust framework.

For interoperability to work more easily, it would help greatly if the digital versions of these 5 golden credentials were standardized.

This is already happening for passports in the form of Digital Travel Credentials from ICAO and for Driving Licenses through the ISO Mobile Driving License standard.

National ID cards are often accepted for travel, and so might most easily be standardized as Digital Travel Credentials.

Bank Account information is included in many ISO20022 message types. But these do not define a digital credential format. For the purposes of leveraging a bank account as an ID proof, the name, address and date-of-birth of the individual is usually required.

The GSMA Mobile Connect set of specification includes the KYC Match response which contain the data required for a telco account credential but does not define a digital credential format.

Next Step: Explore how National ID cards, Bank Accounts and Telco Accounts can be standardized as Digital Credentials.

6.2 Standards for how credentials are proofed.

Standards for the format and content of credentials are only one part of achieving interoperability through identity policy assessment of credentials stored in the user's wallet.

When determining the use of a credential in an identity assurance policy model, the value it holds in validation and verification models needs to be assessed. So how validation and verification of the credential were done in the trust framework under which the credential was issued (the home trust framework) must be understood.

Our analysis has found that trust frameworks use common approaches to validation and verification. Whilst we have managed to categorise the approaches into methods, the detail of how each method is carried out in each framework is different and is documented in framework specific guidance on proofing.

To enable interoperability, standardization of these approaches should be considered.

The following common validation methods have been identified:

Validation Method	Existing Standards
Digitizing Documents – Human Assessment	
- Video with User - Visible Security Features by person remotely, liveness check	
- Face to Face - Visible Security Features by appropriately trained person	PRADO guidelines
Digitizing Documents – Machine Assessment	
- Video with User - Visible Security Features by machine, liveness check	
- Static Picture - Visible Security Features by machine, liveness check	
- UV/IR Security Features (If present)	PRADO guidelines
- Haptic/tactile security features (if present)	
- Crypto read of chip	ICAO
- Validated using a government / framework approved reader	
Logon to Account	
- Crypto Validation e.g., PSD2/SCA logon	

Data	
- Validated against authoritative source	
- Validated against credible source	
Directly Issued Digital Credential	
- Issued directly from authoritative source	

As can been seen from the above table, there are very few standards for validation methods at the moment.

The following common verification methods have been identified:

Verification Method	Existing Standards
Person to Document Image – Human Assessment	
- Image against Photo from ID Document - Face to Face	FISWG Minimum Training Criteria for Assessors Using Facial Recognition Systems [i.22] or for more extensive description the ENFSI Best Practice Manual for Facial Image Comparison [i.23], Appendix A.
- Image against Photo from ID Document - By Person Remotely	
Person to Document Image – Machine Assessment	
- Image against Photo from ID Document - Biometric by Machine - basic	Liveness: PAD measures in compliance with **ISO/IEC 30107-3 [3].** The PAD should be evaluated according to **ISO/IEC 19989-3 [i.18]** BIN-8.4.2-08: Test results for the PAD shall achieve an APCER (attack presentation classification error rate) as defined by **ISO/IEC 30107-3 [3]** at the level of industry best practice. Test results for the PAD should achieve BPCER (bona fide presentation classification error rate) as defined by **ISO/IEC 30107-3 [3]** at the level of industry best practice. NIST's face recognition vendor test guidance
- Image against Photo from ID Document - Biometric by Machine - enhanced	ISO/IEC TR 29156:2015 ISO/IEC 19795-1 [i.17] NIST's face recognition vendor test guidance
- Image against Photo from ID Document - Biometric by Machine - Controlled Capture	
- Validated using a government / framework approved reader	
Logon to Account	
- Logon to Online Service	
Directly Issued Digital Credential	
- Issued directly from authoritative source	

One Time Code	
- One time code to verified account	
Vouching	
- Vouching	

There are more existing standards in the verification space, however most of these are focused on image capture and matching; whilst frameworks refer to these standards they do so in an inconsistent way and these standards only cover part of the image capture and matching process.

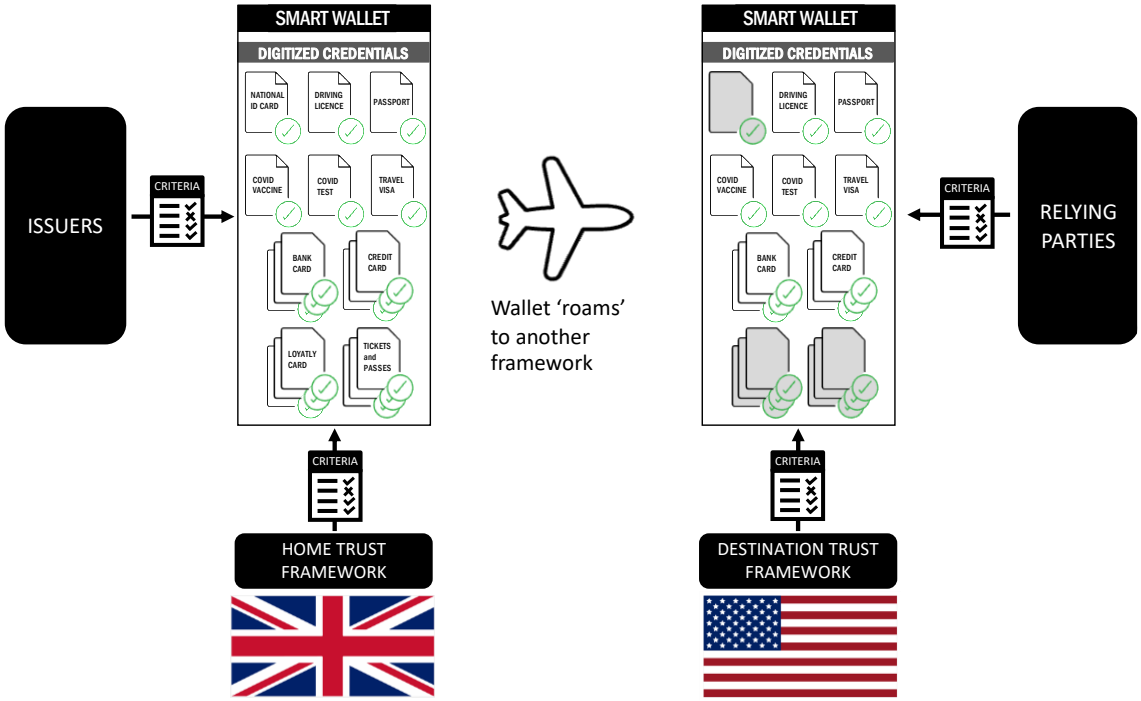
Many of these methods exist because the validation and verification approach is to assess (and digitise) an existing physical document. This is often done by a third party such as a government agent or private sector proofing service, rather than the authoritative source of the document.

The practice of direct digital credential issue from an authoritative source is likely to grow, and if the responsibility of identifying the individual to whom the credential is issued lies with the authoritative source, then the proofing provenance of directly issued credentials is simpler; we simply trust the authoritative source has got this right. If this is the case, then the long term need for standardization of some of the other techniques will reduce as they will become redundant. But will all authoritative source approaches to identifying to whom a digital credential is being issued be sufficiently robust? We have already seen fraudsters obtaining mobile driving licenses in the US, so it may be necessary to consider standards around user-proofing prior to direct credential issue as well.

Next Step: Consider which Validation and Verification methods should have a standard created for them, and my whom.

7 ENABLING 'ROAMING' SMART WALLETS

When I visit, access services, or do business in another country I want the wallet I use on a daily basis to work in that other country, in the same way my phone works as I move from country to country today. I do not want to have to create a new wallet for each new trust domain I encounter. Wallets will need to work across virtual trust domains not just physical countries as our phones need to today. The OCET can be used to enable smart wallets to adapt as they move, or 'roam', from one trust framework domain to another.

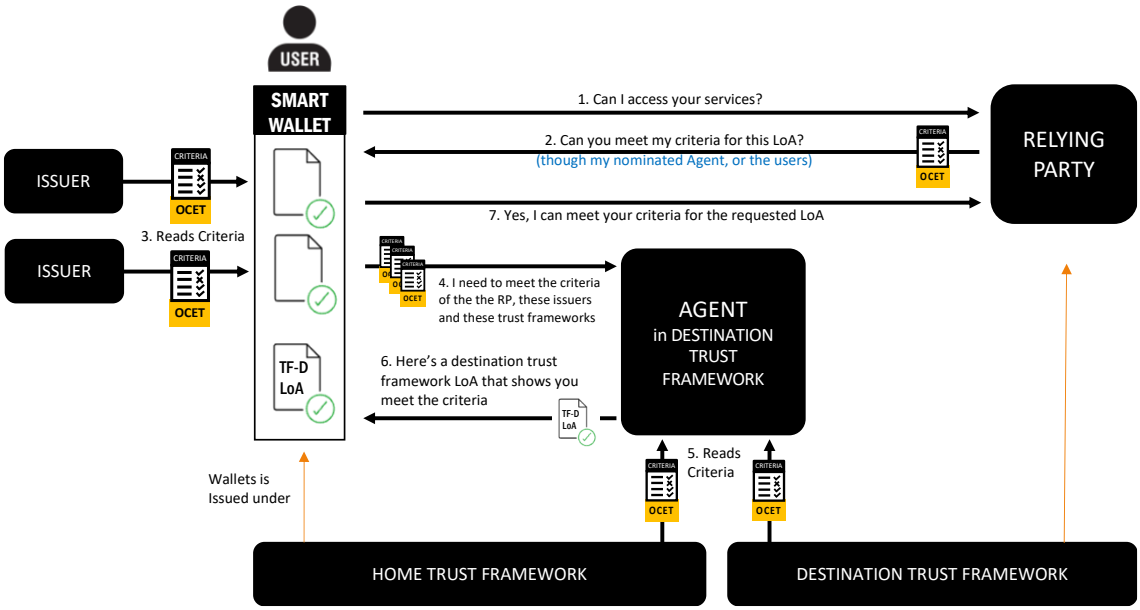


The smart wallet has a particularly challenging role as the interpreter, or assessor, of the polices it is subject to, especially as the wallet 'roams' around the globe. The OCET will allow a wallet to interpret the criteria defined by its home trust framework, stored credentials, any destination trust framework the wallet is roaming into, and from the relying party. The OCET can support expression of policy criteria by all these parties to allow such interpretation.

To achieve scale, Smart Wallets that transcend framework boundaries will need read and dynamically adapt to expressions of policy from all parties.

In the longer term, Smart Wallets are unlikely to be provided by governments (See OIX Governments and Wallets paper). They are more likely to be provided by specialist private sector wallet providers. The OCET can provide a way for trust frameworks to determine whether they trust a roaming wallet and the credentials within it.

Interpretation of local policy criteria will be complex, and we think that Agents who interpret issuer and home and destination trust framework policy criteria to assess compliance, will likely play a key role in interoperability:



Agents might be instructed by the relying party or their trust framework, or on behalf of the user, via their wallet provider. The above diagram shows the wallet passing the issuer policy criteria to the agent; the wallet might only pass a pointer to the issuer criteria to the agent, who will then retrieve them directly from the issuer in the same way that they do from the trust frameworks.

Next Step: Create a proof of concept that explores how a Smart Wallet leverages policy criteria expressed using OCET by different parties as it roams across trust framework domains.

8 MAKING DECISIONS – OCET IN ACTION

In this section we explore how OCET can help support policy criteria acceptability in the decision-making process. We explore how acceptability decisions can be made on a static or dynamic basis, how pragmatism is required when trying to match required policy criteria against those offered by others, and look at some examples of decision making to try and bring this process to life.

Trust Frameworks and Issuers of credentials play the role of **publishers** of policy criteria and can use OCET to express their policy criteria.

Issuers can use OCET to express which criteria a credential complies with and also to set constraints on the use of a credential.

OCET can enable two distinct types of decision making based that leverage this published policy criteria:

- **Static decision making** where a decision on what policy criteria are acceptable is made by human experts and then that decision is itself published as policy criteria.
- **Dynamic decision making** where policy criteria acceptability is determined 'on the fly' based on the policy criteria requirements one or more parties.

Both types of decision making may be applied to in order to achieve interoperability across ID ecosystems. For example, a static decision on which wallets from which frameworks might be made, and then dynamic run-time decisions made on whether credentials in a wallet meet the requirements for the destination trust framework identity assurance model.

8.1 Static decision making

In static decision making, a framework or relying party will use the OCET information published by:

a) another framework to determine which wallets or credential types they will accept,

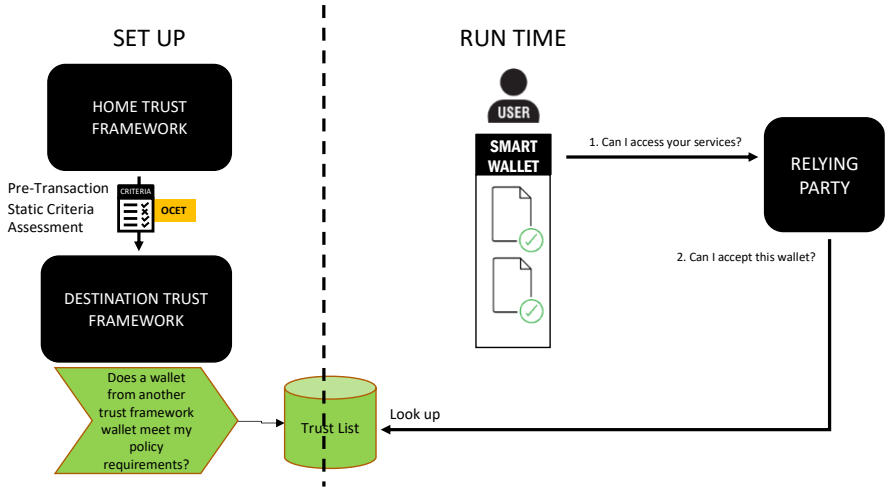
b) by acceptors of credentials – relying parties - to determine which credentials they accept,

The output of a static decision-making process is a declaration of acceptability that is in turn published by the framework or relying party as policy criteria. This might involve for example a framework publishing a list of accepted wallets from another framework, maybe alongside the list of wallets that it certifies directly itself.

To allow systemic acceptance of the wallet, it's acceptance may be published in a 'trust list'. Examples might include:

- I trust wallets from these providers certified by this framework.
- I trust driving licenses from these issuers.

The diagram below illustrates the process for determining whether a wallet is trusted by a framework:



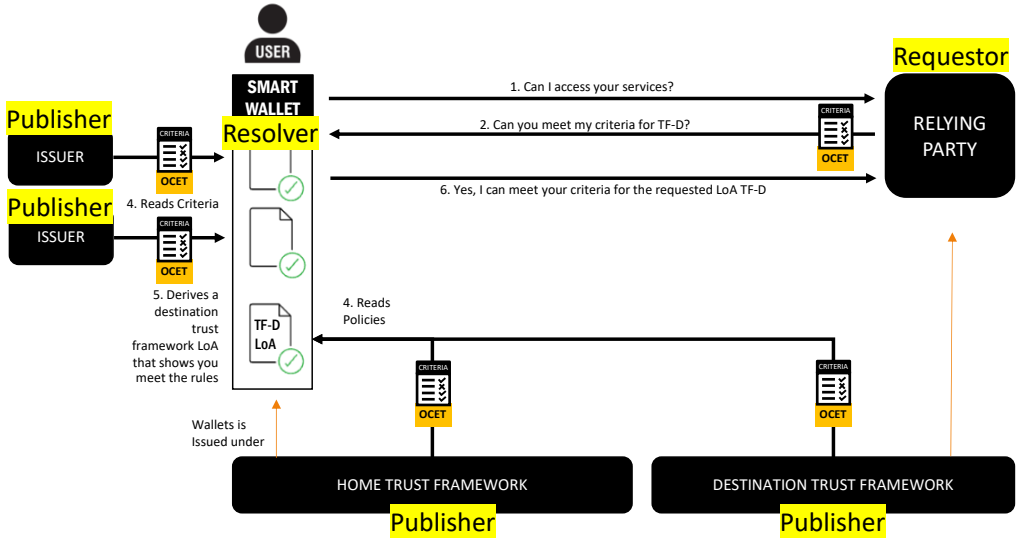
A destination trust framework uses the OCET published policy criteria from a wallets home trust framework to determine whether wallets or credentials from that framework will be accepted within the destination framework. This is done as part of setting up a wallet for acceptance in the destination framework prior to any transaction taking place. When a user then presents their wallet to the relying party who is subject the destination framework, the relying party simply looks up whether they are allowed to trust that wallet from a trust list maintained by the destination framework.

8.2 Dynamic decision making

In dynamic decision making:

- A **requester** – uses OCET to express the policy criteria they will accept. This could be by reference to a prevailing trust framework. Relying Parties will play the role of requestors and will use OCET to express their requirements when asking for credentials or derived information (derived credentials). Wallets will play the role of requestors when an issuer is asked for a credential.
- A **resolver** – determines how to fulfil a request based on the policy criteria in the request and the other published policy criteria the wallet and credentials are subject to. The resolver is the decision-making role. In dynamic decisioning, the wallet, or an agent, will play the role of resolver.

This diagram shows who is playing each role in a typical dynamic wallet request:



The wallet will receive the criteria from the relying party. In this example the relying party is asking for a specific level of assurance from the trust framework is it subject to (LoA TF-D) to be met. The definition of this LoA is from the relying parties trust framework, which from the wallets point of view is the destination trust framework. The wallet it subject to its home trust frameworks policy criteria, which are published using OCET. It must also work to the policy criteria each issuer might publish using OCET around the use of its credential. To resolve whether it can meet the relying parties' criteria, the wallet will read the criteria the relying party is subject to from the destination trust framework, which are also published using OCET. If it can meet the required policy criteria for the level of assurance (for example it contains a passport that was proofed in the correct way to meet the LoA) it can then derive an LoA credential (TF-D LoA) for the user to present to the relying party.

We will explore some examples of relying party requests later in this section.

8.3 Policy Match – Exact or more flexible?

A key activity when making policy decisions is to determine what policy criteria are acceptable. There is a level of pragmatism that policy makers will need to apply when setting acceptable policy criteria; demanding that policy criteria are met exactly by the resolver will make interoperability difficult, as the resolver has to work within the rules of the publishers. A requestor may wish to use a cascade approach to express how closely each required policy criteria is met:

- **Exact:** The policy criteria must meet a one or more exact value from the possible values for that characteristic. For example, security policy must be ISO27001.
- **Range:** The policy criteria can be met by a range of the possible values for that characteristic. For example, security policy can be ISO27001 or SOC2
- **Any:** The policy criteria can be met by any the possible values for that characteristic. Essentially this means that the policy characteristic must be addressed, but the requestor does not care how. For example, there must be an inclusion policy in place, but the details of the policy are not important.
- **Not required:** It does not matter if the policy characteristic is addressed or not, as this policy characteristic is not important to me. For example, it's not important that Tell Us Once is supported.

There will be areas where a wallet can dynamically adapt to policy criteria (e.g., putting up a detailed consent screen and capturing explicit consent), and areas where a wallet cannot adapt to policy criteria (e.g., security standards).

Next Step: Categorize policy criteria wallets can adapt to, vs those that they cannot adapt to.

Next Step: Undertake some use-case based examples of how policy criteria requests might be expressed to validate the cascade approach to characteristic-value matching

8.4 Examples of Published Policy

In this section we explore some examples of how a publisher used OCET to communicate their policy criteria.

8.4.1 Published Policy Example 1 – Trust Framework

Our analysis of the 8 trust frameworks shows in detail how a frameworks can use the OCET to publish their policy criteria. The table below shows examples of how a framework would express its policy criteria using OCET. Frameworks are likely to require their policy criteria are matched exactly:

	CRITERIA			
General Policy Area	Policy Characteristic	Criteria Match Position	Acceptable Values	Rationale
Governance	Certification or Licensing	Exact	Certified directly through framework	
Trust Mark	Display of Trustmark	Exact	RPs must display Trustmark to end users. IDPs must display Trustmark to end users	
Inclusion / Equity / Accessibility	Inclusion Monitoring	Exact	ID Provider has inclusion plan/policy - MUST requirement	
Inclusion / Equity / Accessibility	Accessibility Guidelines	Exact	WCAG	
User Account Management -	Account Closure Triggers	Exact	has not followed the terms of use they agreed to. wants to close it. has died. account was created fraudulently	
Liability	Fault – ID Fraud	Exact	Does not address	
Data Management	Privacy	Exact	Parties must publish a Privacy Policy to other parties. Parties must publish a Privacy Policy to end users	
Data Management	Consent Approach to Data Listing	Exact	Actual Data Listed	

Data Management	Porting data from one IDP to another	Exact	Refers to local DPA legislation = REQUIRED	Not important in a local transaction for my RPs. Important for user only.
Data Management	Right to be forgotten approach	Exact	Refers to local DPA legislation = REQUIRED	No right to be forgotten in my local regulation.
Risk and Incident Management	Quality Management Policy Accepted	Exact	ISO9001	
Fraud Management	Types of IdP Fraud Controls	Exact	Known Fraud sharing. Shared Risk Signals Device Risk Anomaly / Velocity Detection Behavioral Risk	
Fraud Management	Scope of Data / Signals Sharing	Exact	Within Home Framework boundary	
RP requirements	RP flow down conditions	Exact	Ensure RP supports the management of fraud. Prohibited processing rules - no profiling.	
RP requirements	RP Registration	Not Required		
Prohibitions	ID Prohibited Data Uses	Not Required		
Technical and Security Policy	Security Policy Accepted	Exact	ISO27001	
Trust Registry		Not Required		Leave to schemes
Credential Standards	Storage Standards	Any		
Credential Standards	Online presentation Standards	Exact	OIDC4VPs	

8.4.2 Published Policy Example 2 – Credential Issuer

The following example shows how an issuer of a credential would use OCET to declare the policy criteria associated with a mobile driving license. The credential issuer would use OCET to declare some criteria that apply to the credential itself, and to communicate the Identity Assurance Model criteria used to create and bind the credential. Again, when using OCET to publish policy criteria the 'match position' adopted by credential issuers is most likely to be exact.

	CRITERIA			
Identity Assurance Policy Area	Policy Characteristic	Policy Criteria Match Position	Acceptable Values	Rationale
Required Claims	Verified Claims	Exact	Name Address Birthdate DL Number	
Valid Credentials	Credential Type	Exact	Driving License	
Valid Credentials	Credential Format	Exact	mDL	
Valid Credentials	Issuer Type	Exact	Government Agent	Third party scans of physical ID documents are OK
Valid Credentials	Issuer	Exact	Issuers URI	
Validation	Validation Method	Exact	Direct Issue	
Verification	Verification Method	Exact	Direct Issue	
Authenticators	Authenticators required for Presentation	Exact	Face Biometric	
General Policy Area	Policy Characteristic	Policy Criteria Match Position	Acceptable Values	Rationale
Liability	Fault – ID Fraud	Exact	Fault based. In the event of ID Fraud, cap $5,000	
Data Management	Consent Approach to Data Listing	Exact	Actual Data Listed - Masked with user reveal	
Data Management	Porting data from one IDP to another	Exact	Explicitly states this must be supported	
RP requirements	RP flow down conditions	Exact	Prohibited processing rules - no profiling	

Credential Standards	Storage Standards	Exact	mDL	
Credential Standards	Online presentation Standards	Exact	mDL	

8.5 Examples of using OCET in a Request

The following examples explore how a requestor might formulate a request to a wallet using OCET.

8.5.1 |Request Example 1 - Does a Wallet meet my criteria?

This example explores how a request might be formulated to express the policy criteria that make a wallet acceptable to a requestor.

The request could be formed as part of the static decision process as a back-office tool to allow reasoning about wallet acceptability.

Or it could be used dynamically by a resolver wallet (or agent) to determine if the wallet can meet the policy criteria required.

The request would detail the acceptable general policy criteria that the wallet or credential must be able to meet. The example below uses only a selection of the 75 characteristics to illustrate how this process would work. The policy criteria match position column shows how the cascade model above might be used:

	CRITERIA			
General Policy Area	Policy Characteristic	Policy Criteria Match Position	Acceptable Values	Rationale
Governance	Certification or Licensing	Exact	Certified directly through framework	
Trust Mark		Not Required		Local brand trust for user
Inclusion / Equity / Accessibility	Inclusion Monitoring	Not Required		If the user has got as far as presenting an ID, they have been included in their home framework
Inclusion / Equity / Accessibility	Accessibility	Any		
User Account Management -	Account Closure Triggers	Range	has not followed the terms of use they agreed to. wants to close it. has died.	
Liability	Fault – ID Fraud	Exact	Fault based in the event of ID Fraud, cap $10,000	
Data Management	Privacy	Range	Parties must publish a Privacy Policy to other parties. Parties must publish a Privacy Policy to end users	
Data Management	Consent Approach to Data Listing	Exact	Actual Data Listed - Masked with user reveal	

Data Management	Porting data from one IDP to another	Not Required		Not important in a local transaction for my RPs. Important for user only.
Data Management	Right to be forgotten approach	Not Required		No right to be forgotten in my local regulation.
Risk and Incident Management	Quality Management Policy Accepted	Any		
Fraud Management	Types of IdP Fraud Controls	All		
Fraud Management	Scope of Data / Signals Sharing	Any		
RP requirements	RP flow down conditions	Range	Ensure RP supports the management of fraud. Prohibited processing rules - no profiling.	
RP requirements	RP Registration	Any		
Prohibitions		Not Required		
Technical and Security Policy	Security Policy Accepted	Exact	ISO27001	
Trust Registry		Not Required		Will add wallet to own trust registry once the acceptance criteria are passed.
Credential Standards	Storage Standards	Any		
Credential Standards	Online presentation Standards	Exact	OIDC4VPs	Destination framework rule that all RPs received data in OIDC4VP format.

A wallet might be able to adapt to some criteria of the destination framework, even though they are not a requirement of its home framework. For example, a wallet could add masking on data fields when presented for user consent to meet destination framework criteria even if this is not a requirement of its home framework. Or it could be presented via OIDC4VP, even though SAML is used in its home framework.

The step of determining whether a wallet meets the requestors criteria is a pre-cursor to testing whether credentials in the wallet can meet the requestors criteria. Credential acceptance is explored in the next 3 examples.

8.5.2 Request Example 2 – Does a credential meet my criteria?

In this example we look at how a requestor who wishes to hire a car to the end user might express their acceptable policy for a **driving license** using OCET:

	CRITERIA			
Identity Assurance Policy Area	Policy Characteristic	Policy Criteria Match Position	Acceptable Values	Rationale
Required Claims	Verified Claims	Exact	Name, Address, DoB, DL#, Entitlements, Endorsements	
Accepted Credentials	Credential Type	Exact	Driving License	
Accepted Credentials	Credential Format	Exact	mDL	
Accepted Credentials	Issuer Type	Exact	Government Agent	
Accepted Credentials	Issuer	Any		
Validation	Validation Method	Range	F2F, Scan, Direct Issue	
Validation	Validation Methods Combination	Range	Direct Issue F2F + Scan	
Verification	Verification Method	Range	F2F, Selfie Biometric, Direct Issue.	
Verification	Verification Method Combination	Range	F2F Selfie Biometric Direct Issue.	
Authenticators	Authenticators required for Presentation	Exact	FIDO Std	
General Policy Area	Policy Characteristic	Policy Criteria Match Position	Acceptable Values	Rationale
Credential Standards	Online Presentation Standard	Exact	mDL	

The requestor is not looking for a level of assurance so that part of the Identity Assurance Policy model is not used.

They are looking for a credential they can trust, so how it is validated and verified is important.

The type of issuer and who the issuer is will also be important to the requestor, so we have added these to the assurance policy model is in this example.

At the point of requesting specific credentials, there may also be general policy area criteria that apply in the context of this credential, an example is shown at the bottom of the table.

8.5.3 Request Example 3 – Can the wallet derive an attribute I require?

In this example we look at how a requestor who wishes to determine a user is **over 18** express their acceptable criteria using OCET, ensuring that selective disclosure is applied so that the receive the minimum data necessary:

	CRITERIA			
Identity Assurance Policy Area	Policy Characteristic	Policy Criteria Match Position	Acceptable Values	Rationale
Required Claims	Verified Claims	Exact	Over 18	
Accepted Credentials	Credential Type	Exact	Driving License, Passport, National ID	Governments issued credentials
Accepted Credentials	Credential Format	Range	mDL, DTC	
Accepted Credentials	Issuer Type	Range	Government Agent Third Party	Third party scans of physical ID documents are OK
Accepted Credentials	Issuer	Any		
Validation	Validation Method	Range	F2F, Scan, Direct Issue	
Validation	Validation Methods Combination	Range	Direct Issue F2F + Scan	
Verification	Verification Method	Range	Selfie Biometric	Must be the persons face to unlock to proof of age to prevent the use of another person's ID
Verification	Verification Method Combination	Range	Selfie Biometric	
Authenticators	Authenticators required for Presentation	Exact	Face Biometric	
General Policy Area	Policy Characteristic	Policy Criteria Match Position	Acceptable Values	Rationale
Credential Standards	Online Presentation Standard	Exact	OIDC4VC	
Credential Standards	Face to Face Selective Disclosure Standards supported	Exact	Selective Disclosure for JWTs (SD-JWT)	

At the point of requesting specific credentials, there may also be general policy area criteria that apply in the context of this credential, an example of specific approaches to selective disclosure is shown at the bottom of the table.

8.5.4 Request Example 4 – Can the wallet derive an LoA I require?

In this example we look at how a requestor who wishes to receive a particular LoA for a user express their acceptable criteria using OCET. We consider the LoA a derived credential, per the OIX trust framework model, so that is the type of credential requested:

	CRITERIA			
Identity Assurance Policy Area	Policy Characteristic	Policy Criteria Match Position	Acceptable Values	Rationale
Required Claims	Verified Claims	Exact	Name, Address, DoB	
Accepted Credentials	Credential Type	See Assurance Policy Model for the Destination Trust Framework for IAL2		
Accepted Credentials	Credential Format			
Accepted Credentials	Issuer Type			
Accepted Credentials	Issuer			
Validation	Validation Method			
Validation	Validation Methods Combination			
Verification	Verification Method			
Verification	Verification Method Combination			
Authenticators	Authenticators required for Presentation	Exact	AAL2	
General Policy Area	Policy Characteristic	Policy Criteria Match Position	Acceptable Values	Rationale
Credential Standards	Online Presentation Standard	Exact	OIDC4VP	

The assurance policy model for the destination trust framework for IAL2 would be read by the resolver, and may look like the below:

	CRITERIA			
Identity Assurance Policy Area	Policy Characteristic	Policy Criteria Match Position	Acceptable Values	Rationale
Accepted Credentials	Credential Type	Range	National ID Card, Passport, Telco	
Accepted Credentials	Credential Format	Range	mdL, DTC	

Accepted Credentials	Issuer Type	Range	Government Agent Direct Issue	Third party scans of physical ID documents are OK
Accepted Credentials	Issuer	Any		
Validation	Validation Method	Range	F2F, Government Approved Reader, Data	
Validation	Validation Methods Combination	Exact	F2F, Government Approved Reader + Data	
Verification	Verification Method	Range	F2F	
Verification	Verification Method Combination	Range	F2F	

8.6 OCET in Action – further exploration

These examples explore some typical options that exist in the real world where OCET could be leveraged. To refine our thinking and the OCET we want to explore how this will work in more detail, with our trust framework partners, as a key next step.

Next Step: Test how a resolver can map a requestors' criteria to a home and destination trust framework through a deeper desk-top analysis. Use the above use cases of hiring a car, proving age and opening a financial account. Do this in collaboration with framework representatives who are involved in the programme using real policy criteria for those frameworks. This will explore the validity of the cascade approach and help normalize the draft characteristics and values identified so far.

8.7 OCET Publication and Evolution

In the paper we have illustrated what the OCET is and how it can be used in both static and dynamic decisioning situations by various parties. We highlight several next steps to refine the OCET which we will execute over the next 6-9 months. Once the OCET is proven further OIX's intention is to publish it as an open tool for all to user to enable digital ID interoperability across the globe.

OIX's Global Interoperability working group will continue to explore and evolve the OCET in the short term through use of member funds. If OIX is to continue to refine, evolve and publish the OCET a sustainable scalable business model will need to be found to fund this on an ongoing basis.

Next Step: Explore business models to progress and maintain OCET for the benefit of the parties who will leverage it.

9 CONCLUSION

Trust frameworks around the globe follow the same approach, they cover many of the same policy areas and within those areas address the same policy characteristics, albeit with a range of different value settings. They have a common Digital ID DNA.

As part of this common Digital ID DNA, they also approach the key area of Identity Assurance through a common methodology. Whilst some frameworks the use of the methodology is simple and involves the digitization of a real-world ID credential, for others it is more complex involving the examination of various pieces of trusted evidence to determine an overall level of trust, or assurance, for a user.

However, each trust framework is necessarily different and will remain so to meet local legal, policy and technical approaches. We must respect these differences, not try to normalize them.

To help trust frameworks with different DNA, and other parties, to reason around interoperability at a policy level we have created the Open Criteria Exchange Tool (OCET). This allows any party to express the permitted values for a particular policy characteristic as policy criteria.

Trust frameworks might use OCET to reason around interoperability in bilateral discussions. However, we think bilaterals have limited scale; to achieve interoperability on a global scale we need to be able to dynamically assess the policy criteria in play at any one time.

We see the future as a world where roaming-wallets can adapt to the policy criteria of the destination trust frameworks and relying parties they encounter, whilst respecting the policy criteria that have been applied by issuers to the credentials they hold and the criteria of their home trust framework. These truly will need to be smart wallets.

Levels of Assurance might also be dynamically formulated leveraging the ‘golden credentials’ that are carried in the user’s wallet: National ID Cards, Passports, Driving Licenses, Bank Accounts and Telco accounts. To do this, we will need globally recognized standards for these credentials and how they are proofed.

In conclusion: we have proven that frameworks are common enough for interoperability to be possible, but the permutations of their DNA are complex. We do not expect frameworks to entirely normalize to a common set of policies, they are necessarily different.

OIX will support interoperability through enabling expression of policy criteria through OCET and calling for common standards for key credentials.

10 SUMMARY OF NEXT STEPS

The following table groups the next steps highlighted throughout this document into focus areas that the OIX Global Interoperability working group will progress over the next stage of this programme:

Focus Area	Next Step
Refining Trust Framework Digital ID DNA Analysis and OCET	Work with participating trust frameworks to see if any normalization/sub-division of characteristics and values is possible and identify which are most important when considering interoperability. Do this as part of use case-based policy applicability analysis.
	Categorize policy criteria wallets can adapt to, vs those that they cannot adapt to
	Further analysis on authenticator standards referenced by trust frameworks and consideration of standards required (existing and new) to enable interoperability.
	Test how a resolver can map a requestors' criteria to a home and destination trust framework through a deeper desk-top analysis. Use the above use cases of hiring a car, proving age and opening a financial account. Do this in collaboration with framework representatives who are involved in the programme using real policy criteria for those frameworks. This will explore the validity of the cascade approach and help normalize the draft characteristics and values identified so far.
Standards	Explore how National ID cards, Bank Accounts and Telco Accounts can be standardized as Digital Credentials.
	Consider which Validation and Verification methods should have a standard created for them, and my whom.
Technical	Create a proof of concept that explores how a Smart Wallet leverages policy criteria expressed using OCET by different parties as it roams across trust framework domains.
	Explore what a machine-readable format of OCET might look like. Consider which existing technical specifications could be extended to communicate this format.
Business Models	Explore business models to progress and maintain OCET for the benefit of the parties who will leverage it.

It you are interested in getting involved in these next steps, please get in touch with OIX to find out how you can join the working group.