The Laws of Identity in the era of Ubiquitous Identity

Nat Sakimura

Chairman

OpenID Foundation

identiverse

#identiverse

Kim Cameron's

Laws of Identity

1 User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent.

2 Minimal Disclosure for a Constrained Use

The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

3 Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4 Directed Identity

A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5 Pluralism of Operators and Technologies

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6 Human Integration

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7 Consistent Experience Across Contexts

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

(Source) Kim Cameron: Laws of Identity (2005), <https://www.identityblog.com/?p=352>

Identity = set of claims made by one digital subject about itself or another digital subject

(Source) Kim Cameron: Laws of Identity (2005)

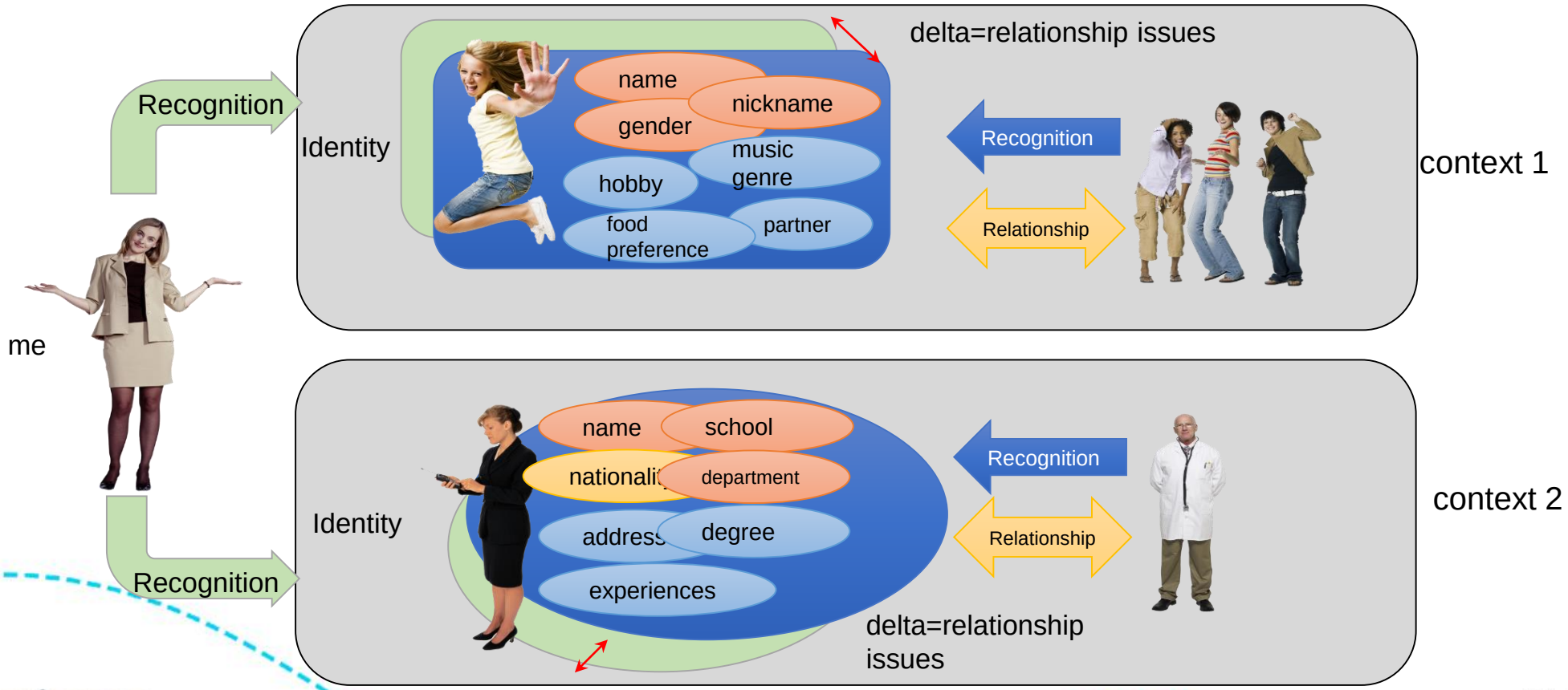
structured and machine readable

Digital Identity = **Digital set of claims made by one digital subject about itself or another digital subject**

(Source) Kim Cameron: Laws of Identity (2005)

Good relationships are maintained with selective disclosure

To create good relationships, we control claims that we constantly adjust what we share within the context to minimising the delta between the recognition by oneself and the counterparty



(Source) Nat Sakimura: Identity and privacy (2011)

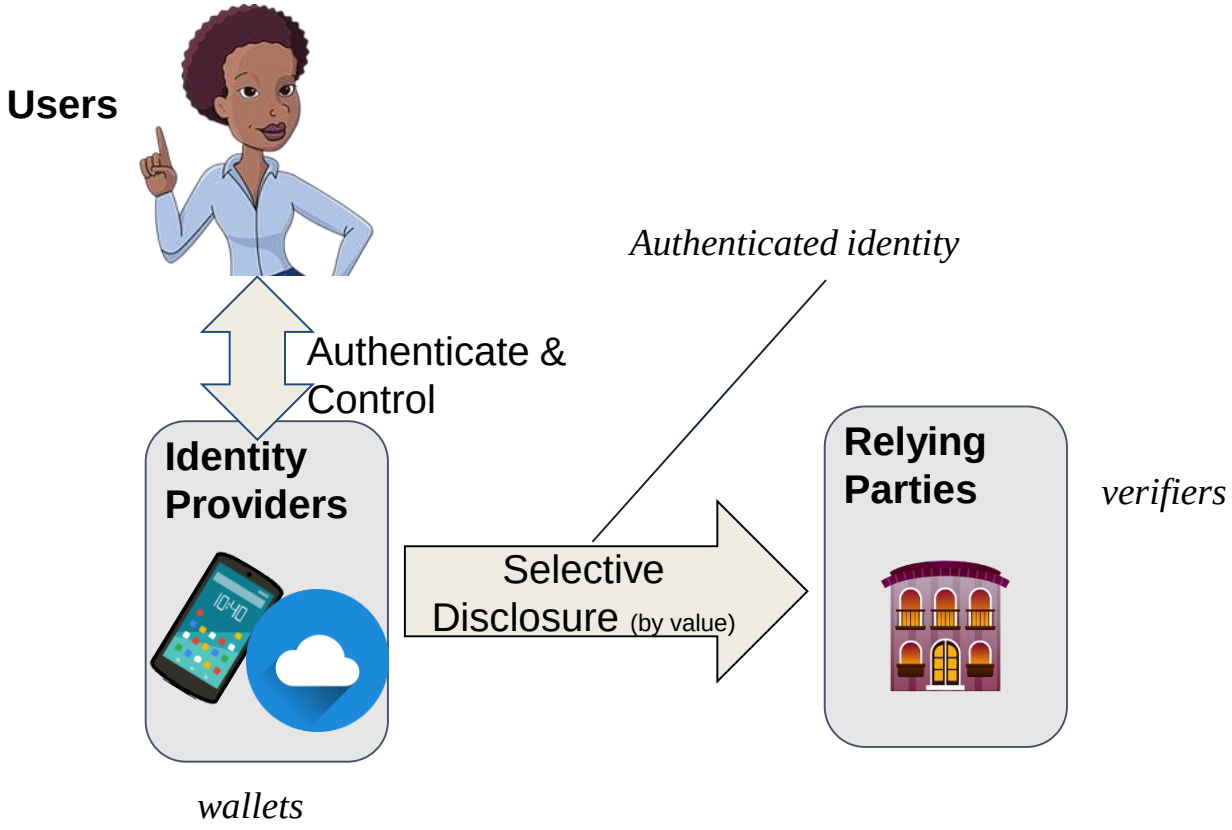
Good relationships keep us happier and healthier. Period.

What makes a good life? Lessons from the longest study on happiness

44,897,338 views | Robert Waldinger • TEDxBeaconStreet

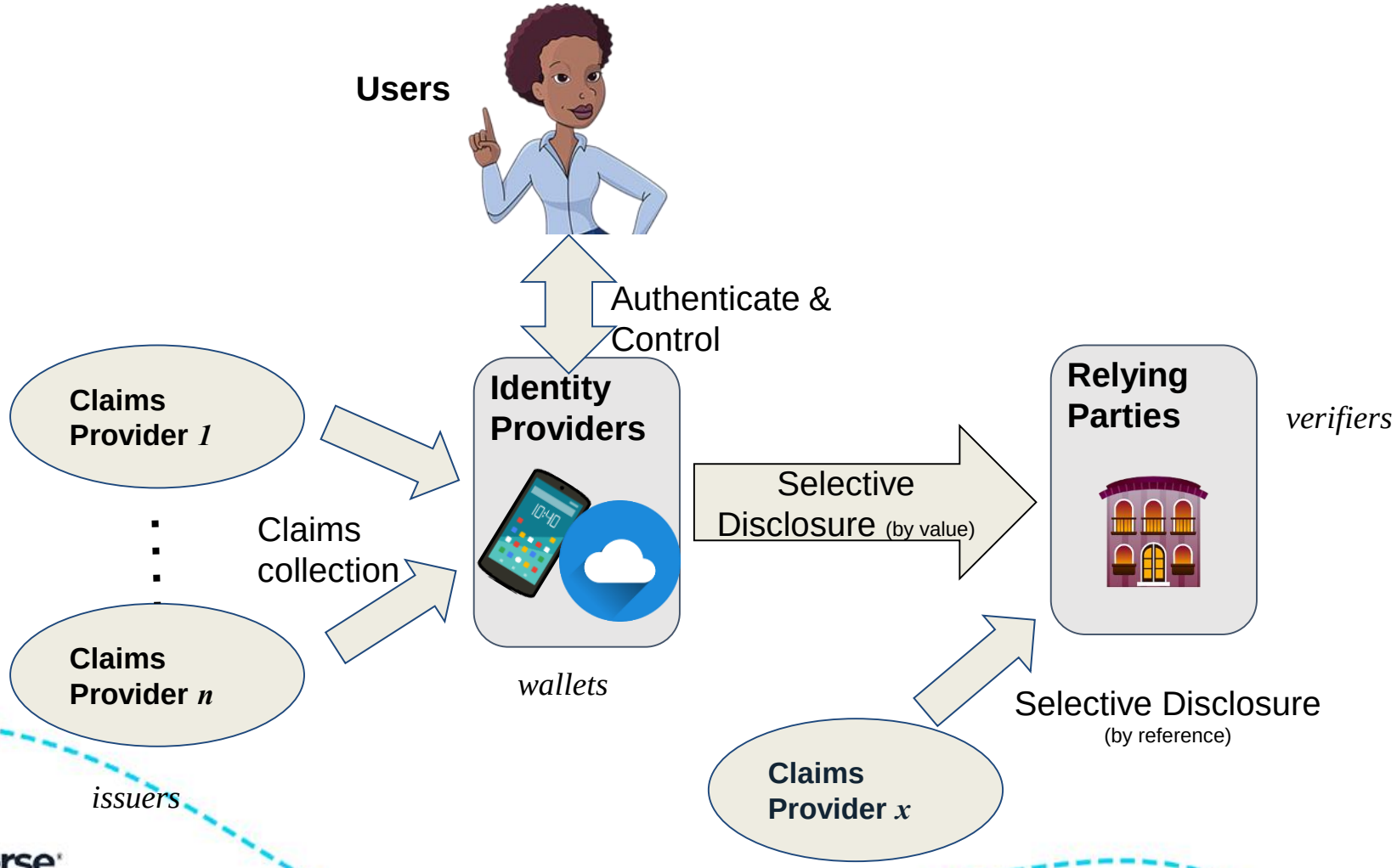
(Source) TED. https://bit.ly/3WpUIFI

You could provide self-attested claims only



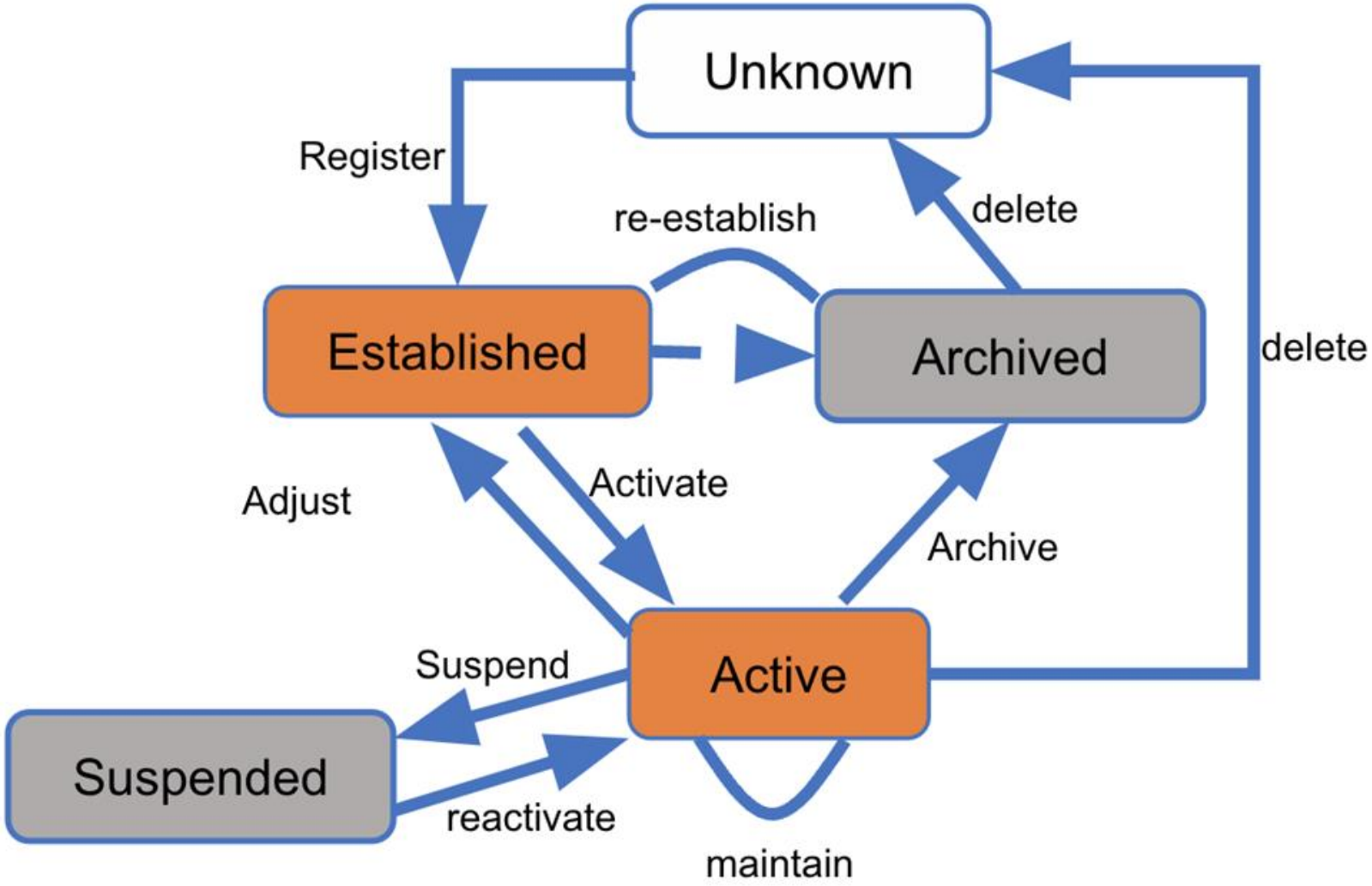
(Source) Nat Sakimura: To do list of SIOP (2019)

but often you may want to provide third party attested claims as well



(Source) Nat Sakimura: To do list of SIOP (2019)

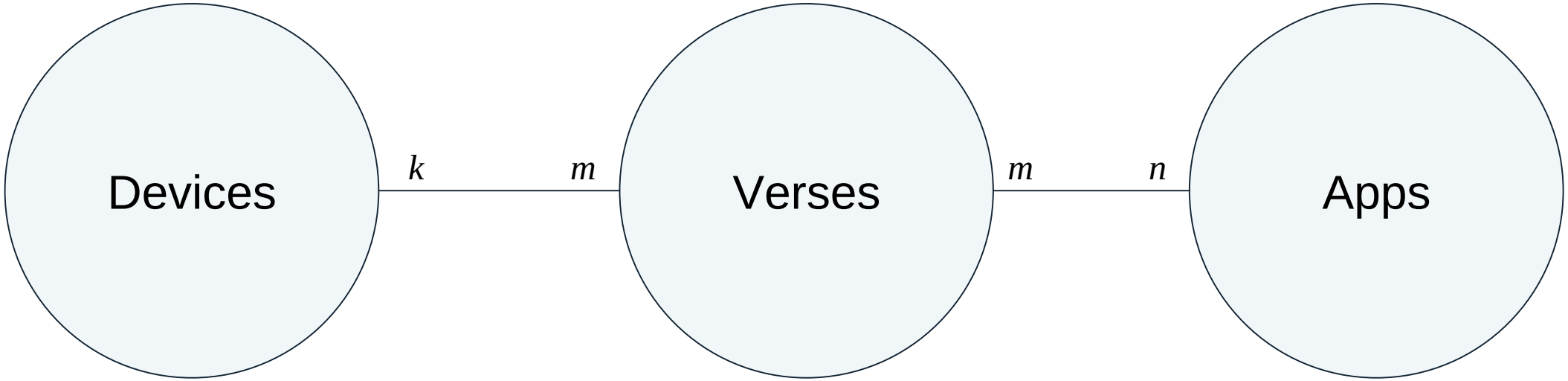
Identity Lifecycle



Ubiquitous identity

single digital identity that can be used across multiple applications and devices

(Source) KuppingerCole (2013) https://www.kuppingercole.com/blog/kearns/pervasive-and-ubiquitous-identity



Ubiquitous Identity implies …

- Multi-device
- Multi-verse / locations
- Multi-applications

- cloud-based ;
- I/F standardised;
- optimised U/I for each use case.

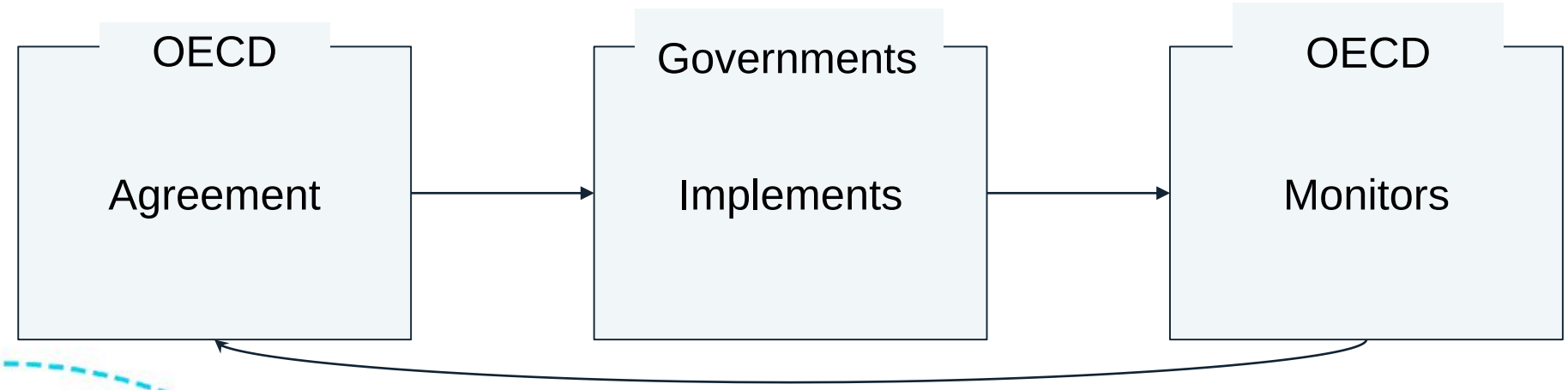
OECD and OECD Privacy Guidelines

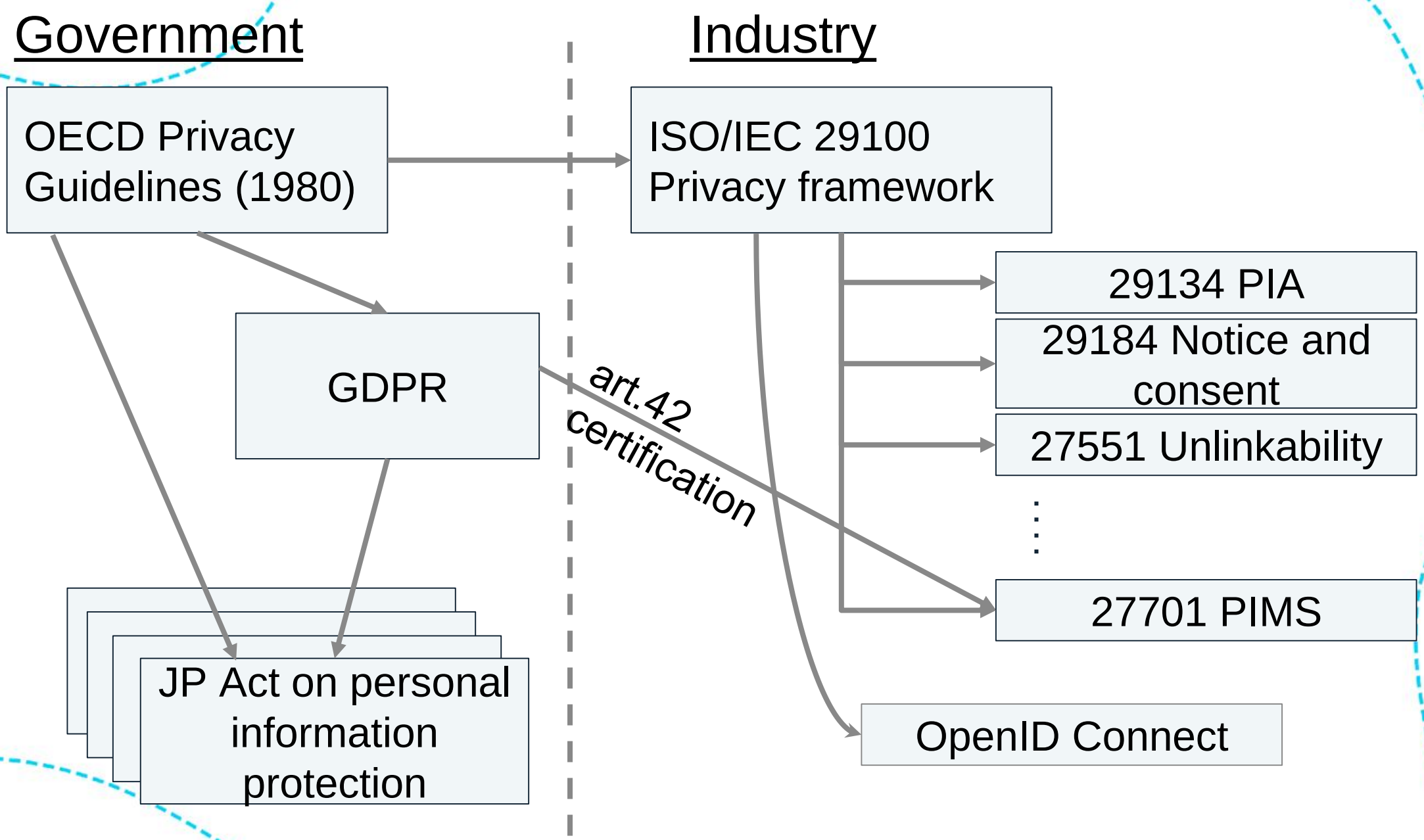
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

bit.ly/3X71YQX

OECD — Organisation of Economic Cooperation and Development

Creates legals instruments upon which member countries are bound to implement the policy in one way or another. Progress will be monitored.




Government
Industry
OECD Privacy Guidelines (1980)
ISO/IEC 29100 Privacy framework
GDPR
art.42 certification
29134 PIA
29184 Notice and consent
27551 Unlinkability
27701 PIMS
JP Act on personal information protection
OpenID Connect

OECD Privacy Principles (1980) [1/3]

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

OECD Privacy Principles (1980) [2/3]

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

OECD Privacy Principles (1980) [3/3]

Individual Participation Principle

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him within a reasonable time;
  at a charge, if any, that is not excessive;
  in a reasonable manner; and
  in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

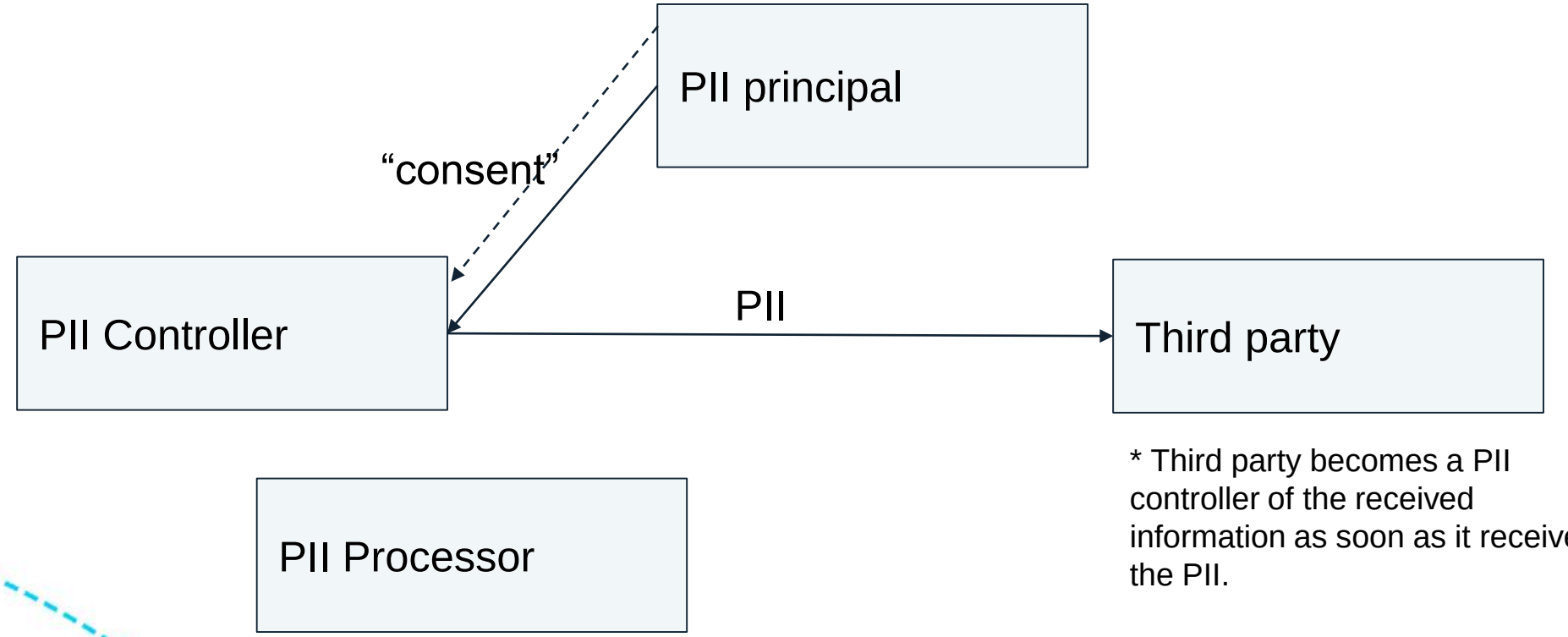
Overview of ISO/IEC 29100 Privacy framework

https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip

bit.ly/3EFdqw5

Overview of ISO/IEC 29100

1. **actors** (PII principal, PII controller, PII processor, third party); and **roles** (PII provider, PII recipient)



* Third party becomes a PII controller of the received information as soon as it receives the PII.

Overview of ISO/IEC 29100

2. interactions; (explains 8 scenarios and role of the actors)
3. recognizing PII;
4. privacy safeguarding requirements;
   - derived from four factors:
     - 1) Legal and regulatory, 2) Contractual, 3) Business, 4) Others (incl. preferences)
5. privacy policies; (internal & external)
6. privacy controls.
7. ISO/IEC 29100 Privacy Principles

ISO/IEC 29100 Privacy principles is a more detailed version of OECD Privacy Principles

ISO/IEC 29100 Privacy Principles	OECD Privacy Principles
1 Consent and choice	4 Use Limitation
2 Purpose legitimacy and specification	3 Purpose Specification
3 Collection limitation	1 Collection Limitation
4 Data minimization 5 Use, retention and disclosure limitation	4 Use Limitation
6 Accuracy and quality	2 Data Quality
7 Openness, transparency and notice	6 Openness
8 Individual participation and access	7 Individual Participation
9 Accountability	8 Accountability
10 Information security	5 Security Safeguards
11 Privacy compliance	

OIDC was created ISO/IEC 29100 in mind

ISO/IEC 29100 Privacy Principles	ISO Standards	OpenID Connect
1 Consent and choice	ISO/IEC 29184 ISO/IEC 27556	prompt=consent
2 Purpose legitimacy and specification	ISO/IEC 29134	policy_url
3 Collection limitation	ISO/IEC 27701	scope/claims, PPID, ephemeral sub
4 Data minimization 5 Use, retention and disclosure limitation	ISO/IEC 29184 ISO/IEC 27555	(RP management. Documented at policy_url)
6 Accuracy and quality	ISO/IEC 27701	(realtime nature, trust framework)
7 Openness, transparency and notice	ISO/IEC 29184	policy_url
8 Individual participation and access	ISO/IEC 27701	(OP and RP policies)
9 Accountability	ISO/IEC 27701	(Trust framework)
10 Information security	ISO/IEC 27701	formal verification, (Trust framework)
11 Privacy compliance	ISO/IEC 27701	(Trust framework)

but wait! What unlinkability?

The protocol itself is said to be unlinkable if its executions cannot be linked, given explicit settings for the adversary and target entity role.

Naming convention for notions of unlinkability

RP + AP – U unlinkability

Adversary

Target entity

(source) based on ISO/IEC 27551 Figure 2

There are 8 notions of unlinkability!

Notions of unlinkability	Adversarial role(s)	Target role(s)	Explanations
Passive outsider (PO-U)	PO	U	Attempt to track U across authentications while these are being monitored (read-only)
Active outsider (AO-U)	AO	U	Attempt to track U across authentications while these are being controlled (read-write)
RP-U	RP	U	The RP attempts to track the U across authentications. (anonymous)
AP-U	AP	U	The AP attempts to track the U across authentications.
RP+AP-U	RP and AP	U	The colluding RP and AP attempt to track U across authentications.
AP-RP	AP	RP	The AP attempts to track the RP across authentications. (Tracking by an IdP)
AP-RP+U	AP	RP and U	The AP attempts to track the pair (U, RP) across authentications.
RP+RP'-U	RP and RP'	U	Colluding RPs attempt to track the U across authentications. RP may be able to track U in transactions with RP, but cannot track the same U communicating with RP'. (PPID)

(source) Based on Table 1 of ISO/IEC 29551

The Laws of Identity

Mapping Laws of Identity and Privacy Principles

Laws of Identity
1. User Control and Consent
2. Minimal Disclosure for a constrained Use
3. Justifiable Parties
4. Directed Identity
5. Pluralism of Operators and Technologies
6. Human Integration
7. Consistent Experience Across Contexts

ISO/IEC 29100 Privacy Principles
1 Consent and choice
2 Purpose legitimacy and specification
3 Collection limitation
4 Data minimization
5 Use, retention and disclosure limitation
6 Accuracy and quality
7 Openness, transparency and notice
8 Individual participation and access
9 Accountability
10 Information security
11 Privacy compliance

1 User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent.

- "Consent" under information asymmetry is not really a consent
- Human capability limitation
- Over-consent tendency
- Collection by observation in device context poses challenges

- Privacy Notice
  - OIDC: policy_url
  - OpenID4VP:

- "Consent"
  - OIDC: 3.1.2.4. Authorization Server Obtains End-User Consent/Authorization
  - OpenID4VP: The Wallet also authenticates the End-User and gathers consent to present the requested Credentials.

2 Minimal Disclosure for a Constrained Use

The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

- Information asymmetry makes it difficult to judge whether the request is minimised.
- In metaverse like context, linking through observation may become much easier than in traditional context.
  - e.g. Carrying a same NFT bag.

- OIDC: Claims parameter.
- OpenID4VP: presentation_definition Parameter

3 Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to **parties having a necessary and justifiable place** in a given identity relationship

- Who judges the “justifiability”?
- Users cannot, in general.
- Trust list?

- Examples:
  - SingPass (OIDC): Singapore government judges if applications/services are justifiable to be able to register the RP.
  - They are also required to register policy_url.

4 Directed identity

A universal identity system must support both “omni-directional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles

- Services have to provide Omni-directional identifiers etc.
  - OIDC: OP Metadata, RP Metadata
  - OpenID4VP: Verifier Metadata

- IdP/Wallets has to be able to provide PPID and K-Anonymity
  - OIDC: PPID
  - OpenID4VP: BBS+?

5 Pluralism of Operators and Technologies

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers

- Competition among the providers.
- They usually support multiple protocols (they have to otherwise, they will not able to migrate to new versions.)
- Standardised interface is a must: otherwise, only the biggest will remain.

- OIDC: Hundreds of thousands of IdPs worldwide.
  - Problems: RPs usually do not accept them but only the top 3 or 4.
- OpenID4VP: Prevention of wallet centralisation should be contemplated seriously

6 Human Integration

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks

- Easy to understand ceremonies across devices and verses.
  - Constrained I/F may pose unique challenges
- Easy to recover from the exception condition
  - e.g. credential not found
- Attack detection

7 Consistent Experience Across Contexts

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies

- A bit challenging in the multi-device, multi-verse context as form factors etc. are different.
  - The intuitive link among the different ceremonies optimised to the devices.

- OIDC:
  - IdP Chooser–Username–Credential–Consent Flow
- OpenID4VP
  - TBD but probably:
  - Wallet Chooser–Credential Chooser–Consent Flow

To close

OECD Draft Recommendation on the Governance of Digital Identity

https://www.oecd.org/gov/digital-government/draft-oecd-recommendation-on-the-governance-of-digital-identity-public-consultation.pdf

bit.ly/42Z63cj

identiverse

Draft Recommendation on the Governance of Digital Identity

Access to essential services across the public and private sectors and trust between individuals, businesses, and governments rely on being able to prove one's identity. Traditional identity verification involves physical proofs such as birth certificates, driver's licenses, ID cards, or passports. However, the digital transformation offers opportunities to consider technology for identity verification both online and offline. Digital channels now offer identity verification processes and access to authenticating verified identity claims through digital credentials and wallets, eID cards, and mobile ID applications.

Despite the benefits of digital identity, in many countries there often remains a lack of cross-sector collaboration, interoperability, and poor-quality user experience. Governments must take a holistic approach that addresses the needs of all stakeholders and focuses on user experience and effectiveness throughout the digital identity lifecycle. There is great variety in governance models for digital identity systems and solutions, which has created fragmented systems of multiple accounts and solutions for governments, businesses, and users to manage.

Establishing a successful digital identity system and widely adopted solutions can simplify interactions, enable personalisation, and reduce the risk of error and fraud. The success of digital identity systems relies on their usability and accessibility by the intended audience, including

THANK YOU!