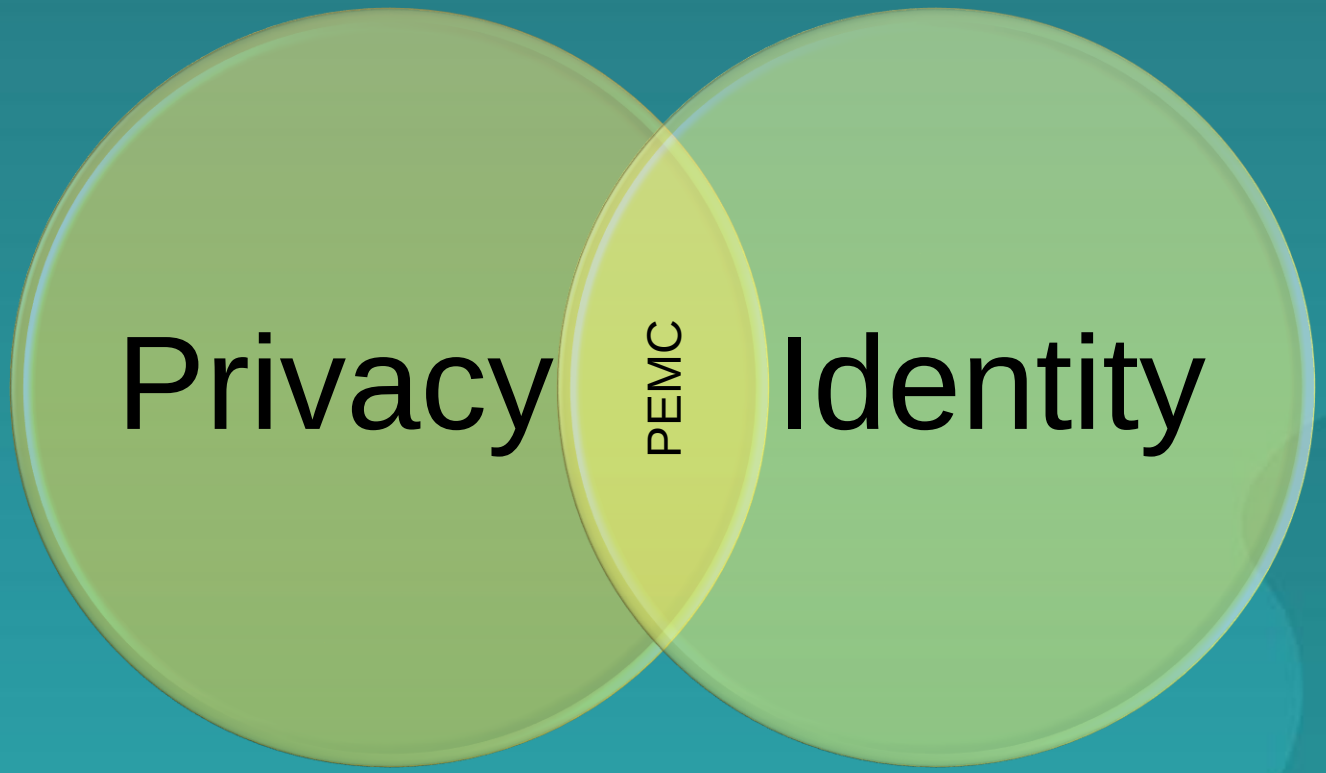
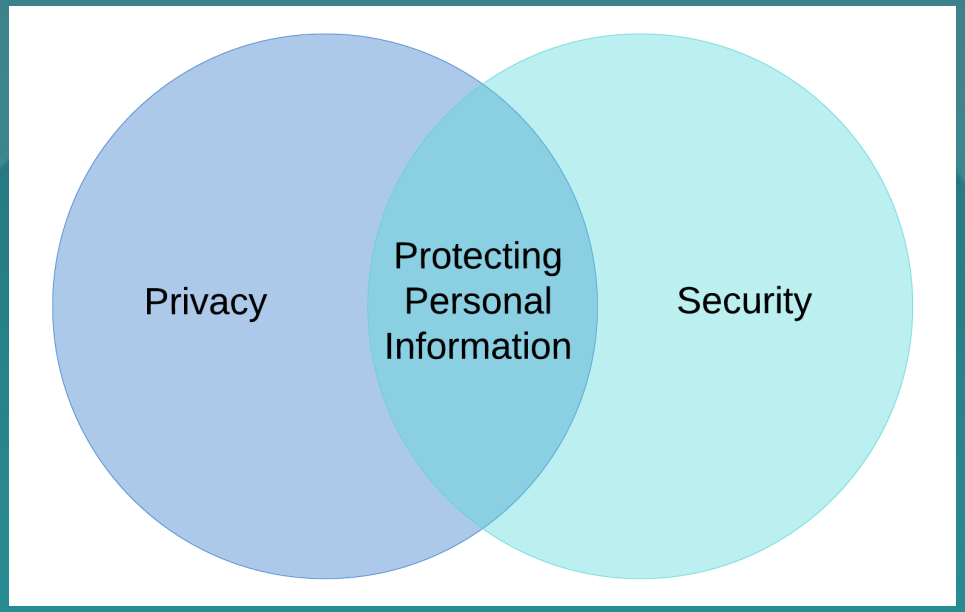
Privacy Enhancing Mobile Credentials

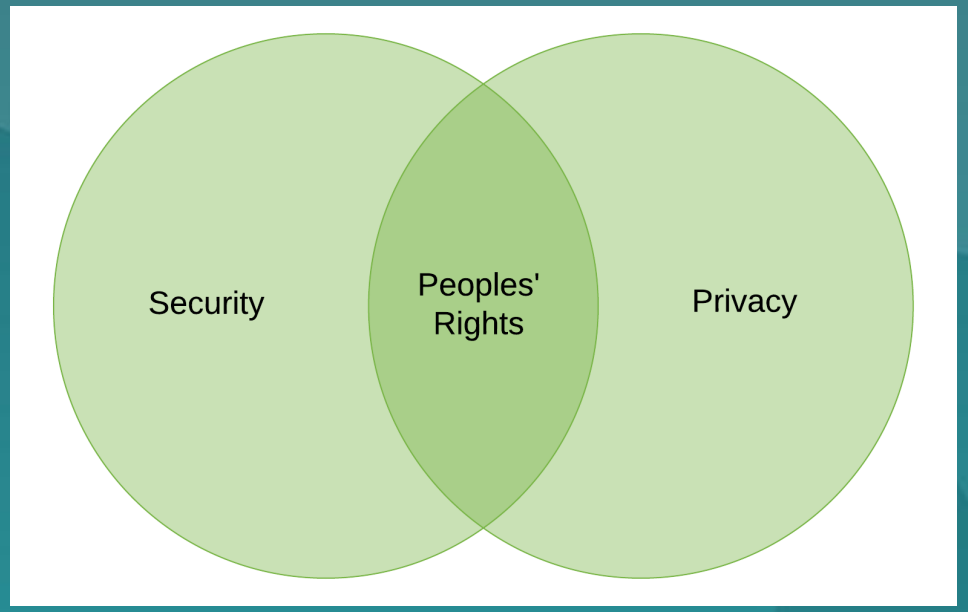
Sal D'Agostino, IDmachines, Kantara Initiative

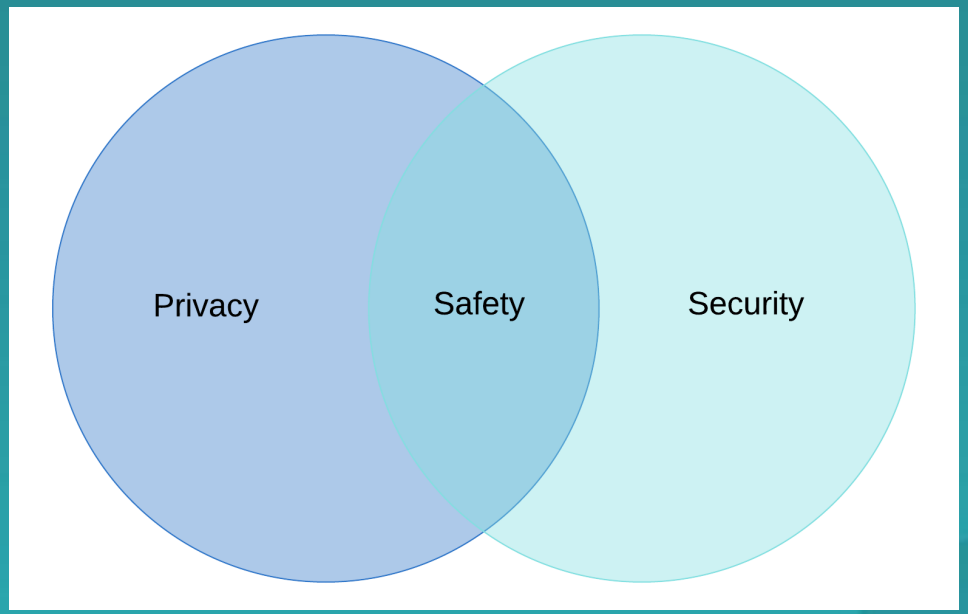
Respecting Privacy And Protecting Identity



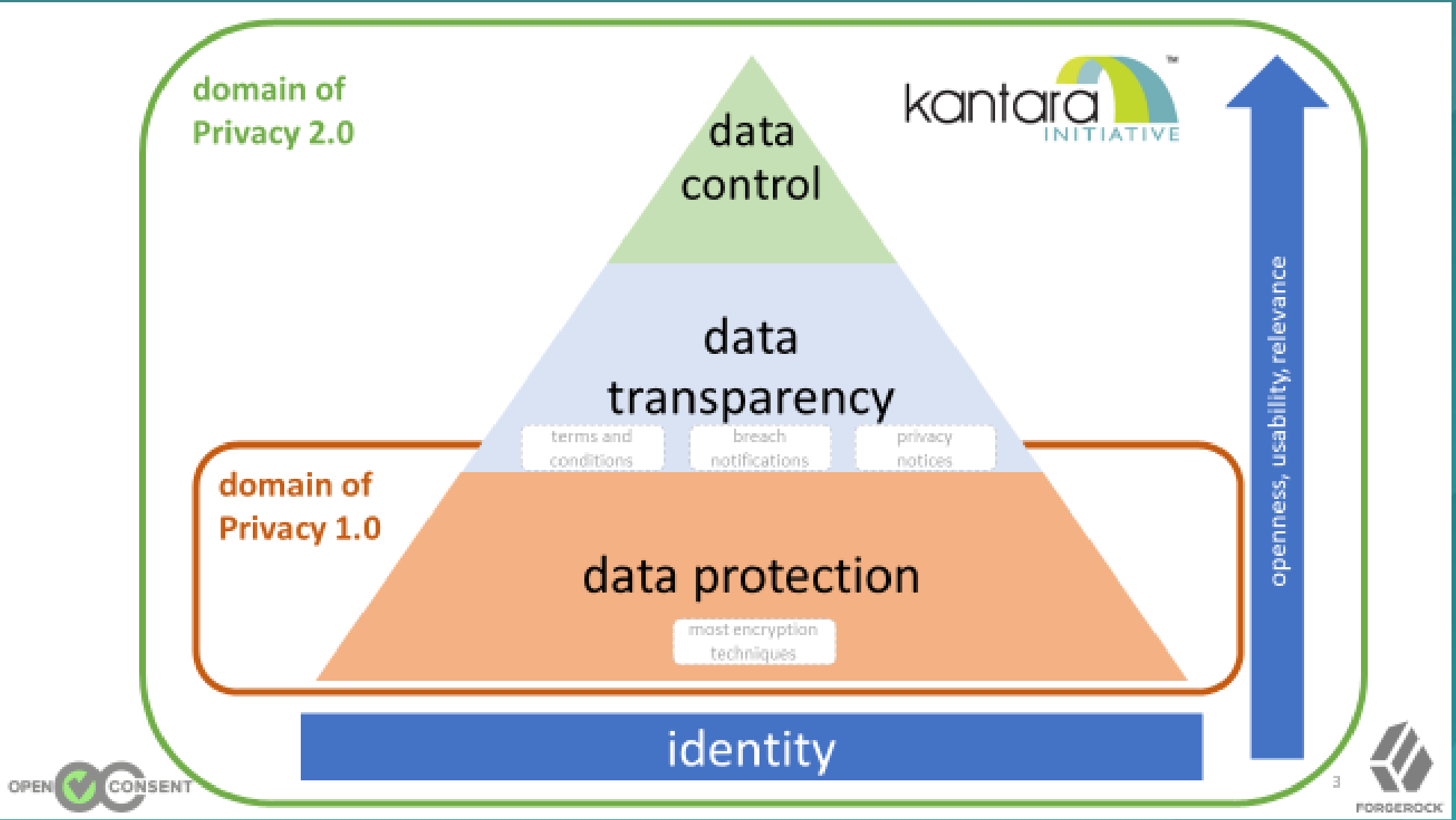
Individuals should be able to choose what they disclose, to whom, and under what conditions


Privacy
Protecting Personal Information
Security


Security
Peoples' Rights
Privacy

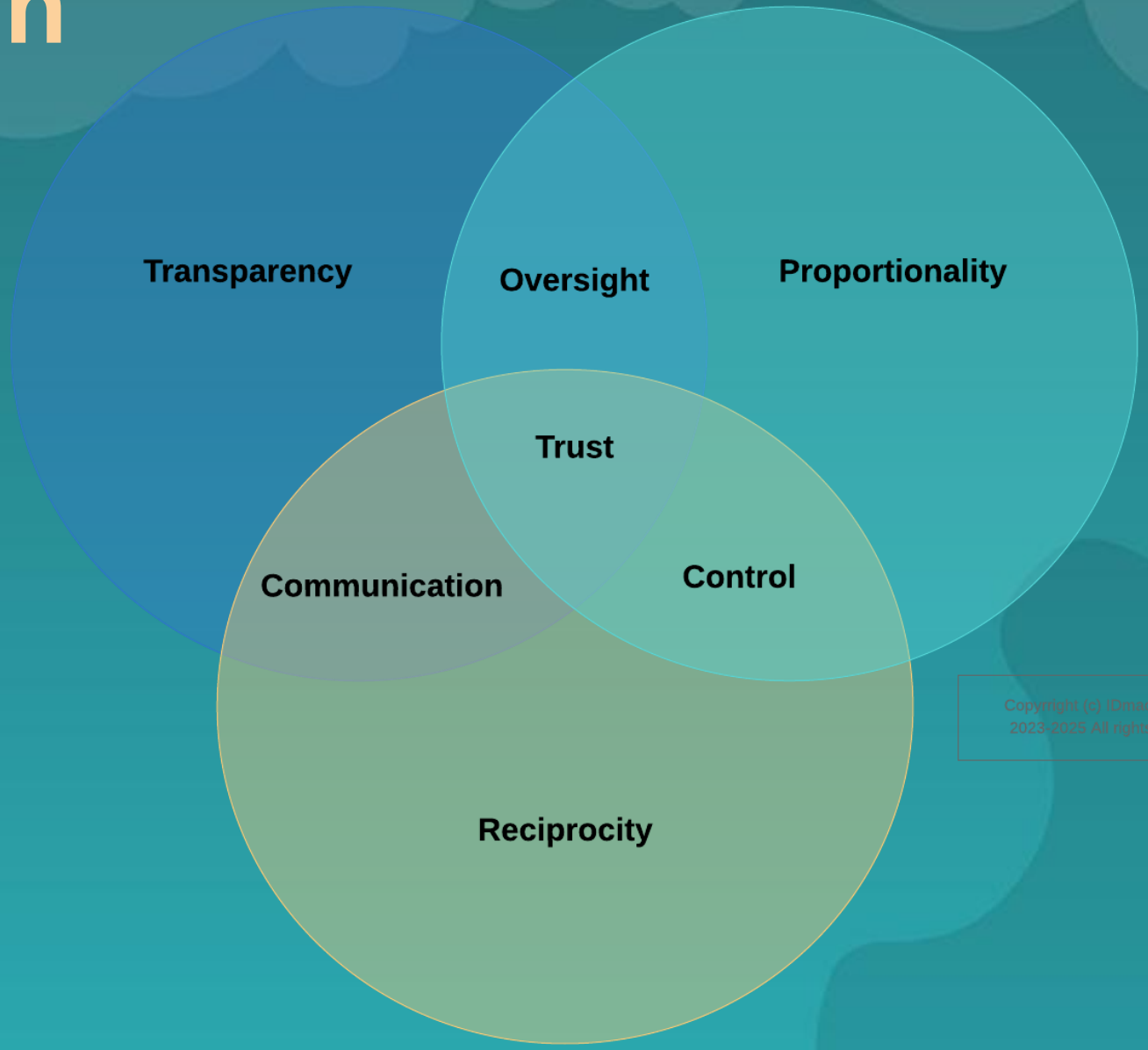

Privacy
Safety
Security

Identiverse 2018



IDmachines

Trust Venn



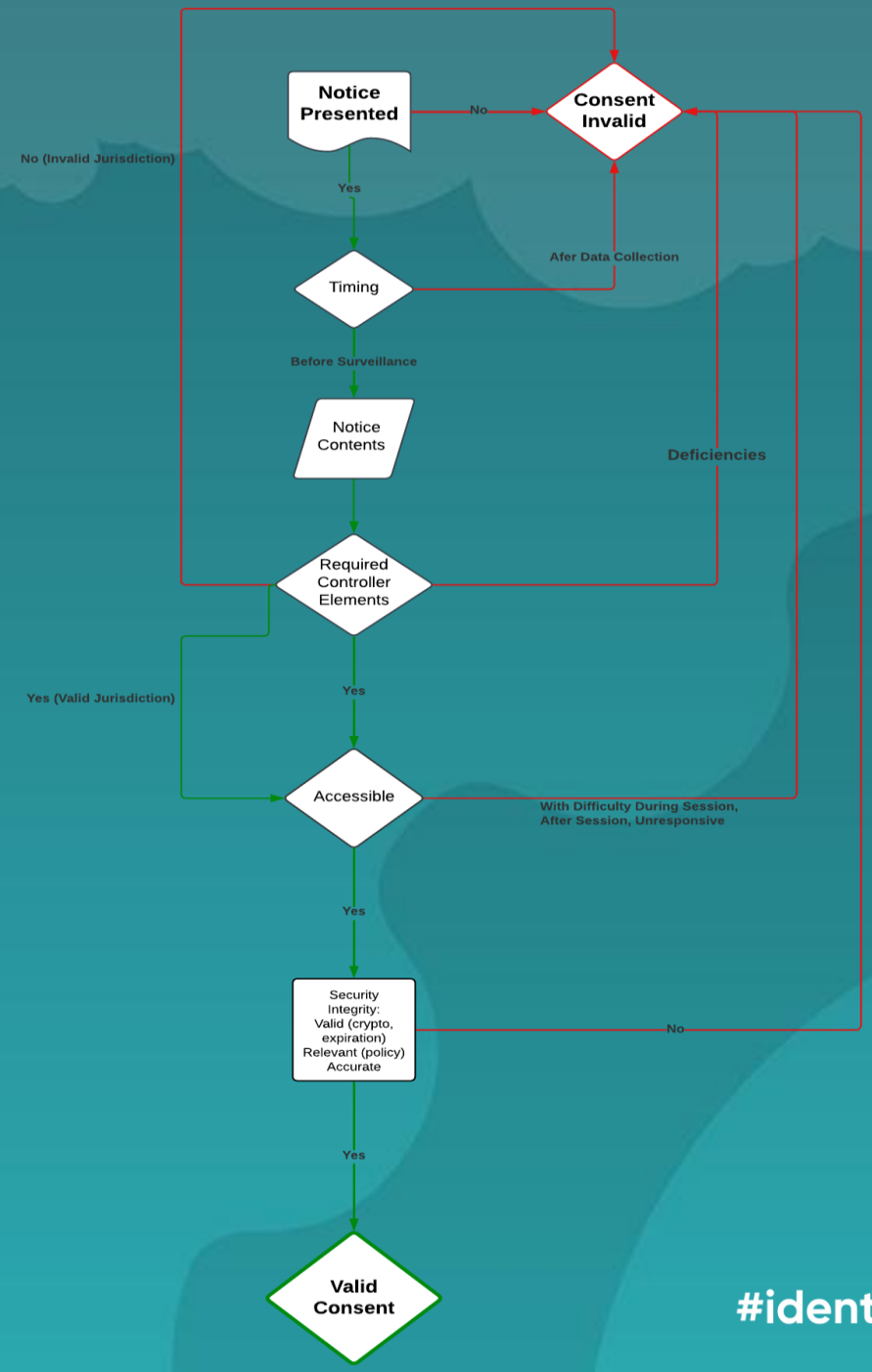
Transparency Performance Report Workflow and Transparency Performance Indicators (TPIs)

TPI 1
Timing of PII Controller Identification

TPI 2
Presence of Compulsory Identification

TPI 3
Security and Privacy Rights Access

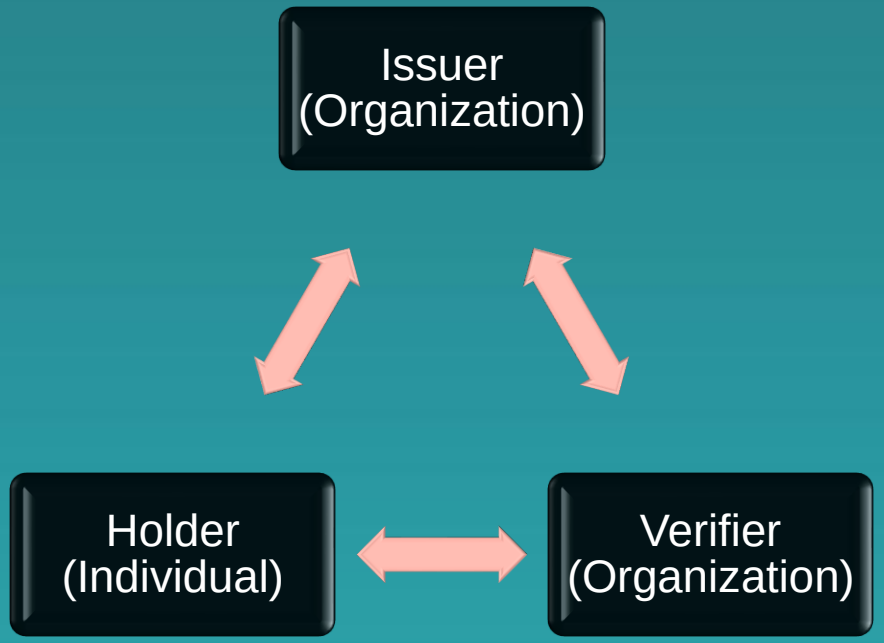
TPI 4
Security and Sovereignty



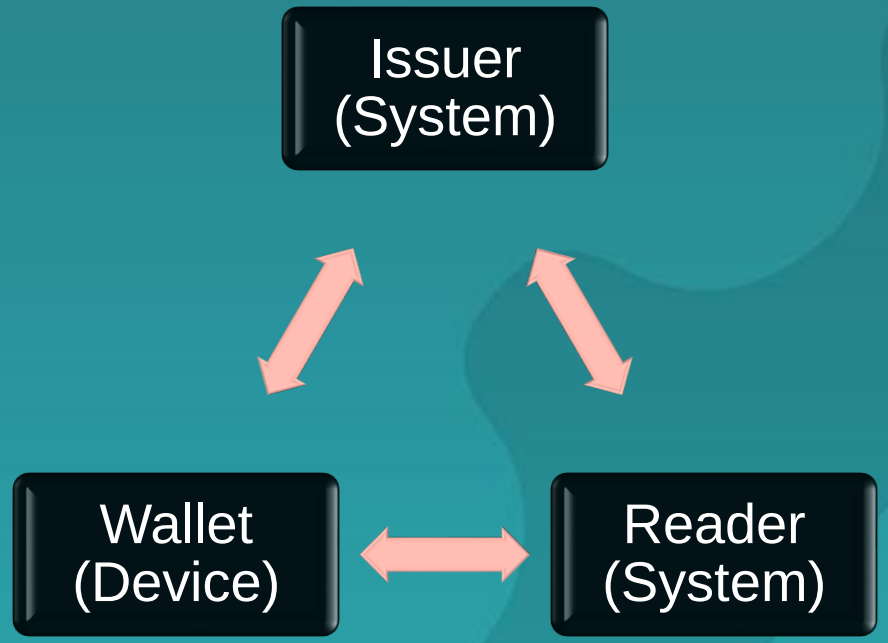
[ANCR Work Group]

A tale of two ‘trusts’

“Trust” between individuals & organizations



Technical “Zero-Trust” between devices



People don’t trust organizations based on their technical security controls

An unequal relationship with our phones.

"We love our phones, but we do not trust them. And love without trust is the definition of an abusive relationship."[1]

[1] From The Conversationalist

Privacy Enhancing Mobile Credentials WG

The purpose of the proposed work-group is to create a set of requirements and conformance criteria to protect the privacy of individuals holding or using mobile credentials such as mobile Driving Licenses. This includes, but is not restricted to, technology ecosystems based on ISO/IEC 18013-5 compliant mobile driving licenses. Existing standards can provide technical and transactional assurances of user choice and data minimization at the point of presentation of the credential, but do not provide assurances to the holders of mobile credentials that relying parties that may collect their identity attributes will use those attributes solely for the fulfillment of the purposes for which the mobile credential was presented. Failing to respect the consent of mobile credential holder or the legal authority of the verifier to collect the identity attributes could violate the privacy of the mobile credential holder.

PImDL Report

- Addressed Privacy for mDL ecosystems

PEMC Guidance Report

- Guidance for Privacy & Mobile Credentials

PEMC Requirements

- Kantara Recommendation

Conformance Testing (in progress)

- Requirements for creating a (Kantara) trust mark (ISO 17065 certification)

PEMC Implementors Guidance

Information for Verifiers

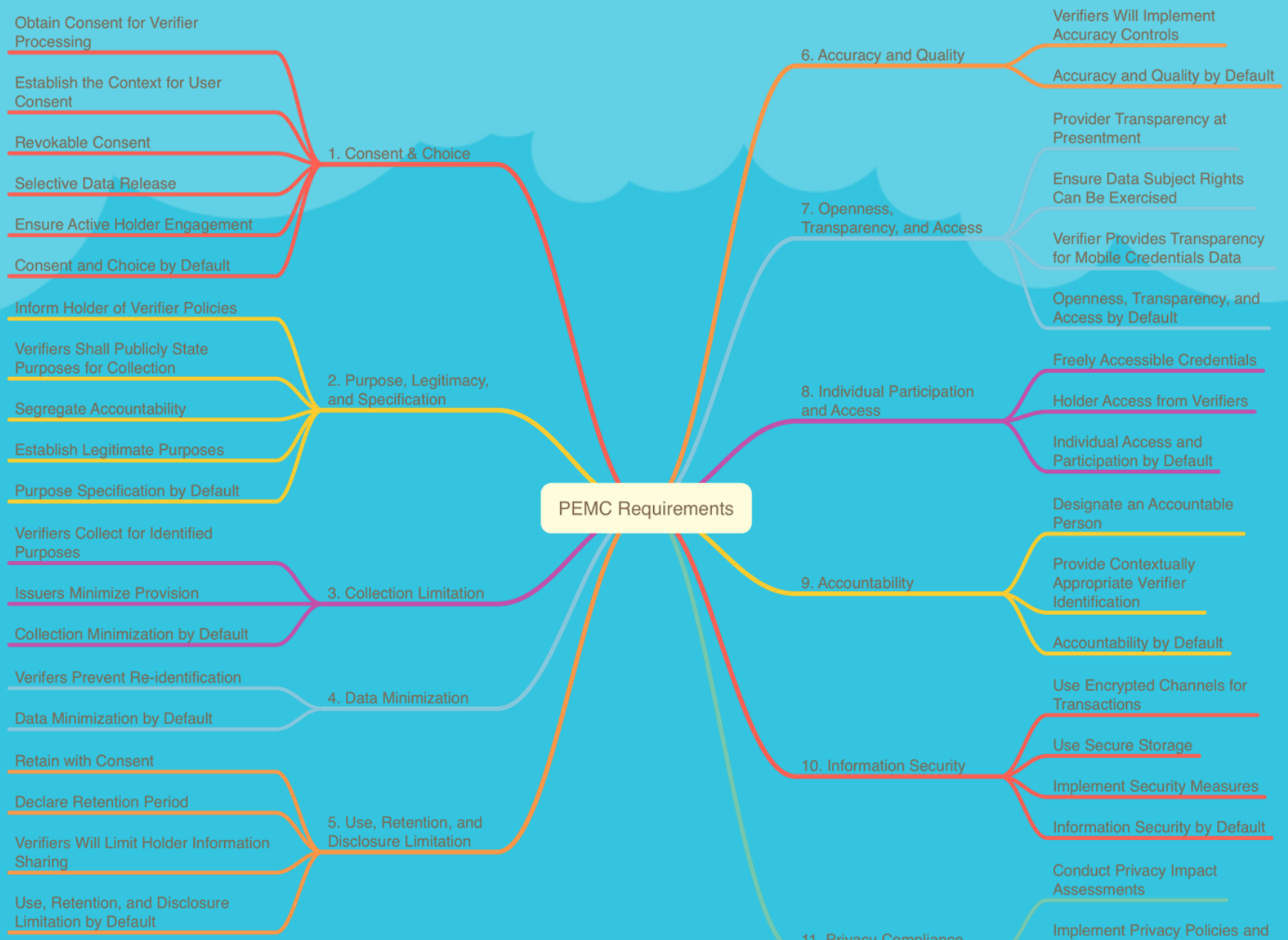
A Verifier organization processes personal data in a particular operational circumstance – the type of business, regulatory requirements, etc.

For a Holder to execute a well-informed choice, the Verifier must identify itself to the Holder/App through appropriate means (e.g., terminal authentication). Before collecting personal information from a Holder, the Verifier must determine (i.e., identify and describe) all aspects of their personal data processing.

Based on the context of any given transaction and this prior determination, the Verifier must determine the contents and type of notice(s) it will share with Holders. In each context the Verifier operates, the Verifier must share the notice(s) as determined and then comply with the requirements of the notice(s) that have been made available to Holders. If the Verifier does this appropriately, the individual who presents their information will not be surprised by the transaction or any subsequent processing of their personal information.

When using a Vendor, a Verifier remains responsible for meeting its obligations in the operational circumstances in which it operates. The Verifier must obtain assurances from the Vendor and make them accessible to the Holder.

- Guidance Follows…


PEMC Requirements
1. Consent & Choice
Obtain Consent for Verifier Processing
Establish the Context for User Consent
Revokable Consent
Selective Data Release
Ensure Active Holder Engagement
Consent and Choice by Default
2. Purpose, Legitimacy, and Specification
Inform Holder of Verifier Policies
Verifiers Shall Publicly State Purposes for Collection
Segregate Accountability
Establish Legitimate Purposes
Purpose Specification by Default
3. Collection Limitation
Verifiers Collect for Identified Purposes
Issuers Minimize Provision
Collection Minimization by Default
4. Data Minimization
Verifers Prevent Re-identification
Data Minimization by Default
5. Use, Retention, and Disclosure Limitation
Retain with Consent
Declare Retention Period
Verifiers Will Limit Holder Information Sharing
Use, Retention, and Disclosure Limitation by Default
6. Accuracy and Quality
Verifiers Will Implement Accuracy Controls
Accuracy and Quality by Default
7. Openness, Transparency, and Access
Provider Transparency at Presentment
Ensure Data Subject Rights Can Be Exercised
Verifier Provides Transparency for Mobile Credentials Data
Openness, Transparency, and Access by Default
8. Individual Participation and Access
Freely Accessible Credentials
Holder Access from Verifiers
Individual Access and Participation by Default
9. Accountability
Designate an Accountable Person
Provide Contextually Appropriate Verifier Identification
Accountability by Default
10. Information Security
Use Encrypted Channels for Transactions
Use Secure Storage
Implement Security Measures
Information Security by Default
11. Privacy Compliance
Conduct Privacy Impact Assessments
Implement Privacy Policies and Procedures
Privacy Compliance by Default

Consent for Verifier Processing Considerations (WG draft)

Informed Decision-Making: Holders must be provided with clear, concise, and easily understandable information about what personal data is being collected, how it will be used, and with whom it might be shared. This information is crucial for them to make an informed choice.

Granular Choices: Where feasible, offer granular options rather than an all-or-nothing approach. This allows Holders to consent to specific processing activities while opting out of others, enhancing their control.
Timing of Consent: Consent must be obtained at or before the point of data processing. It should not be a retroactive justification for data already processed.

Opt-Out Mechanisms: Clear and accessible mechanisms must exist for Holders to opt out of data collection or usage practices. Their decisions to opt out must be respected and promptly implemented by the system.

Cognitive Overload Mitigation: While obtaining explicit consent is paramount, organizations must be mindful of potential "consent fatigue" or cognitive overload on Holders. Continuously prompting for consent for every minor interaction can diminish the effectiveness of the consent process itself. Stakeholders should explore and implement strategies to balance explicit consent requirements with user experience, ensuring that consent requests are meaningful and not burdensome. This involves setting preferences that persist or providing clear explanations of ongoing processing based on initial consent, with easy ways to review and revoke that consent.

Functional preconditions (WG draft)

Data Scope has been documented

The Verifier should explicitly identify and document the personal information elements they intend to request or derive from a Holder's mobile credential. Without knowing what data is involved, it's impossible to design an appropriate consent mechanism or adequately inform the Holder.

Purposes have been identified and documented.

The Verifier should clearly define and document the specific, legitimate purpose(s) for collecting and processing each personal information element or group. Consent must be specific to the purpose(s) for collection. Vague or overly broad purposes invalidate consent. This also forms the basis of the Notice to the Holder.

Functional preconditions (WG draft)

Notice Mechanism has been implemented.

The Verifier has designed and implemented an evident, conspicuous, and easily understandable Notice. This Notice must be presented to the Holder *before or at the point of* requesting mobile credential data and must contain:

- A description of the personal information attributes being requested/processed.
- The purpose(s) for processing.
- The identity of the Verifier (and any relevant third parties the data might be shared with, if applicable, along with purposes for that sharing).
- Information on how the Holder can withdraw consent (if applicable to the specific interaction).
- A link to a more detailed privacy policy, if appropriate

Functional preconditions (WG Draft)

Consent Mechanism has been implemented.

The Verifier has designed and implemented an unambiguous mechanism for the Holder to provide affirmative consent *after* reviewing the Notice. This mechanism must:

- Be separate from other terms or actions (e.g., not bundled with general terms of service acceptance unless directly related and clearly explained).
- Offer an explicit "accept/agree" or equivalent affirmative action.
- Allow the Holder to equally easily "decline/disagree" or abstain from providing the credential data without undue friction (beyond being unable to access the service that requires that data).

Functional preconditions (WG draft)

There is a Consent Record System

The Verifier has a reliable system or process to record the Holder's consent (e.g., timestamp, specific version of notice consented to, scope of consent given).

There is a No-Consent Process

The Verifier has a defined process for scenarios where a Holder withholds consent, ensuring that processing related to the denied consent does not occur and the Holder is appropriately informed of any consequences (e.g., inability to access a specific service).

Staff Training

The Verifier has been trained. Staff who engage with consent systems or processes (e.g., those involved in designing interaction flows, IT staff implementing the systems, and customer-facing staff, if applicable) are trained on this consent requirement and internal procedures.

Tests (WG draft)

Notice Availability & Timing Test

Procedure: Initiate an interaction requiring credential data from the Verifier's system.
Observation: Is a Notice presented before or at the point of data request? Is it easily accessible and readable?
Success Criteria: Notice is timely and presented.

Notice Content Adequacy Test

Procedure: Review the content of the presented Notice.
Observation: Does it accurately list the personal information to be processed? Does it clearly state the specific purpose(s)? Is the Verifier identified? Is the language understandable to a typical Holder?
Success Criteria: Notice content is complete, accurate, and transparent as per pre-conditions.

Consent Action Test

Procedure: Interact with the consent mechanism.
Observation: Does the system require an explicit, affirmative action from the Holder to signify consent (e.g., clicking "Agree," unchecking a pre-filled box is not sufficient)? Can the Holder easily decline?
Success Criteria: Consent requires an explicit, affirmative action. Declining is straightforward.

Tests (WG draft)

Data Processing Post-Consent Decision Test

Procedure:

Scenario A: Provide consent. Attempt to complete the transaction/interaction.

Scenario B: Decline consent. Attempt to complete the transaction/interaction.

Observation:

Scenario A: Does the system process the Holder's data as described in the Notice?

Scenario B: Does the system refrain from processing the Holder's personal information for the purpose for which consent was denied? Is the Holder informed of the outcome of declining (e.g., service unavailability)?

Success Criteria: Data processing aligns with the Holder's consent decision. The system respects denial of consent.

Consent Record Audit:

Procedure: (If backend access or logs are available) After a successful consent interaction, attempt to locate the record of this consent.

Observation: Is a record of consent stored? Does it contain relevant details (timestamp, scope)?

Success Criteria: A verifiable record of consent exists.

Privacy Enhancing Mobile Credentials (PEMC) - Kantara Initiative

JOIN THE PEMC WORK GROUP

Thank you

identiverse®

A CRA Resource