Controller Credential (for privacy rights authorization and engineering)

"The missing link between Human Trust and Digital Trust Assurance" for Human Identity that is Soverign Self (HISS)

Digital surveillance is inherently untrustworthy and ***transparency over surveillance*** is missing for people. Surveillance transparency is necessary to achieve human trustworthiness, and control independent of technology. There is no trust for human tech only trust frameworks for enterprises and tech itself. In the work here privacy is understood as human/individual centric, not business, legal and technical centric. This design rule is critical for trustworthy (including digital identity) infrastructure. For this purpose this task force is tasked with specifying a credential that can be used with and for any identity management technology, including SSI, using International ISO/IEC standards and related Kantara Specifications.

This task force is tasked with the specification of the Privacy Controller Credential for accountable (to the individual) surveillance transparency, providence and accountability.

Process in progress:
 	
1. Updated Jan 6
2. [Proposed] Update to TF Objectives
3. Technical Discussion Points
  a. Linking Records
  b. Providence Fields
  i. Beneficial Owner
  1. Owner Agreement
4. Discussion Papers
  a. Decentralized Data Governance
	Notice & Consent Task Force
	
	Project owner:
	
	Mark Lizar
	
	Editors
	
	Surveillance Controller EditorSalvatore DAgostino
	
	OCA Schema Editor:
		Status
		
		ACTIVE
		
		Spec Dev Link

	Specification proposal: Define the assurance required to extend decentralized semantic governance for dynamic data controls to support privacy and trustworthy/regulated/***surveillance*** a: • Privacy Controller Credential	

Privacy Controller Credential For Decentralized Human ~~Data~~ Surveillance Governance aka Notice and Consent

This working effort specifies a regulatory controller from existing standards that apply and can be mapped to any legal authorization for data processing.

This credential is comprised of the legal entity name and accountability profile as specified by regulation utilizing ISO/IEC 29100 Privacy & Security Techniques. An open (no-fee, no barrier) and international standard from ISO (the Internationational Organization for Standardization) and the IEC (International ElectroTechnical Commission). The use of this standard for the creation of records and receipts is critical for scaleable and interoperable Decentralized Data Governance interoperability between technical domains and legal jurisdictions.

What is this for:

This specification is for the regulation and governance of surveillance and digital identity technology independently of any digital identifiers or trust frameworks. The objective is for the this specification to work with and enhance digital surveillance assurances already provided by work in ToiP. The credentialling process benchmarks the privacy, security and compliance of digital identity technologies with international standards.

The aim of this task force outputs is to create a specification and by so doing implement ISO/IEC international standards to enable regulatory interoperability with human controls and transparency that scale for any authorized surveillance context. To do this, this effort builds upon standards, incorporating additional technical specifications in order to support ToiP community efforts.

Challenges being addressed with the PCC specification have been raised in the Kantara ANCR WG, W3C DPV CG, ISO/IEC 27560 Technical Committee's, CIO Council, DIACC Special Interest Group, IETF GNAP, and VC's with DiD's. The overarching objective is therefore to provide a specification that supports these community efforts.

1. The accountable person may or may not be an employee of the organization.
2. Different jurisdictions name/define and reference this role differently
3. Some jurisdictions, like the UK have a data controller registry (DCR), where this binding is public and legally required (benefit in this case, challenge where absent) and the name of the accountable person is publicly available in ICO DCR. (using blinding identity taxonomy)

4. Some jurisdictions, like the EU require an accountable data controller representative in the jurisdiction where a service is operating, in order to address legal data privacy and security issues that may arise.
5. 2 or more Controllers might be accountable for processing of personal data.
    a. Identify in context of service for any user the controller and accountable person.
6. The privacy law in some jurisdictions, can itself break privacy law in other jurisdictions by requiring the accountable person information to be published publicly,
7. Specifies how to axquire a VC (in this case the Privacy Controller Credential) for trust assurance for privacy assurance
8. Gap of an international notice & control protocol and semantics for governance interoperability between domains and jurisdictions.

Specification Objective

1. Develop an extensible controller credential format.

The specification shall provide:

- a record format that MUST blind the identity of the accountable person,
- be usable as a linked data in a notice of control receipt, which provides only the controller information required for the purpose of credential use.
- record and provide a profile of the bound controller credentials in a manner that can show the controlling person before, during and after the use of a decentralized digital identifier.
- control providence that begins with the person making the assertion to the accountable role using laws and standards to bind privacy rights request to a legal entity.

Decentralized Data Governance

Decentralized Data Governance is the focus of the first Discussion Paper, which aims to look at the overlaps of digital identity surveillance technology and regulator led (regulatory) data governance. This will present the overall architecture and the contribution of certain standards used in the credential, as well as how digital identity specifications and protocols can be deployed to implement decentralized data governance.

Used to make credential

Standards

ISO/IEC 29100

- interop / usable for applying 29184 (as a compliance tool)
- interop with 27560 - Kantara Consent Receipt Work
- future - to use 27560 to interop with 2750 - Privacy by Design
    - pending open access and usability of ISO Spec, e.g. through a Kantara or National Standards body liaison

Specifications

- Kantara ANCR WG, AuthC protocol and V2 Notice Record and Consent Receipt Specification (for implementing the AuthC protocol) (parallel work)
- W3C DPV CG Specification for notice record and receipt semantics

baseline is the international ISO/IEC 29100 security and privacy techniques framework, this is mapped to Legal jurisdiction notice schema and the differences and risks (in terms of rights and the performance of data controls) is provided as a component of the notice of control.

Using the Credential

The use of an international standards framework for providing standarized notice semantics is critical to harmonize or highlight different security, privacy and identity management governance requirements. Standardized semantics, usable for any data governance is also critical for human interoperability /usability across domains which is the key driver of this work and effort at ToiP .

*****