Privacy Controller Credential Specification v.2

Executive Summary

- This specification is for binding transparency and accountability into a credential for decentralized data governance
- This specification uses ISO/IEC standard Format, information structure and W3C DPV semantics to specify a controller notice to enable standard record and receipt for transparency over the processing of each digital identifier based relationship. Doing so by implementing privacy rights to govern and control the use of the personal information end to end, like encryption.

Background

- Create an open international and public specification for access to privacy in digital identity managed profiles and systems
- to enable infrastructure for interoperable data governance - aka - people to independently access privacy rights for personal data control's, transparency and accountability.
    - if extended to SSI architecture enable wallets for micro-credentialing
- Contribute this into a framework of specifications and standards for a conformance suite -
    - ISO/IEC 27560 - Contribution for Notice and Consent code of practice for records and receipts
    - NIST Privacy Framework - rights defaults -
    - W3C Data Privacy Vocabulary - Control Ontology -
    - GNAP and OpenID Connect - FAPI / UMA - Identity Management Protocols
    - ANCR WG: notice record and receipt framework
- specify a standard endpoint for authorization based claims (micro-credentials)

Introduction

In privacy regulations globally the notice and notification requirements in legislation are the most consistent across jurisdictions. In all regulations the identity of the PII Controller is required to be provided to the person before, at the time, or as soon as possible, when processing personal information.

how to extend a conformance notice record to a privacy controller record.

- Stakeholders
    - Regulators
    - PII Controllers

Problem Statement

- Security

Scope of Specification

Specifying these fields and mapping them to both Data Governance Standards and ToiP Architecture.

- Authoritative Providence
    - Organization (legal entity) Standing
        - Legal Status
        - Jurisdiction
            - local, regional, national, international
    - Accountable Person
    - Accountable Role
        - Providence as a professional
            - Employee or 3rd Party
            - Owner - Director (verifiable publicly)
            - Data Protection Officer (qualified)
    - Privacy Access Contact Point - (for dynamic or static data controls)
- Verification and Assurance of Providence
- Validation ?

Policy for Use of the Credential

- Controller Privacy Policy

Operational Privacy (Identity and Security) (Engineering) Design Principles

- Principal of "Transparency, Proportionality, and Control Reciprocity - Dynamic Data Controls"

Privacy Controller Controller Fields

Glossary

Privacy Stakeholders	ISO Definition	
Regulator /		
PII Principal		
PII Controller		
PII Processor		
3rd Party		

References for use for creating a Unified (generic) Data Control Vocabulary for OCA

Standard /Specifications	Title	Description	Resource Status
ISO 29100	Information technology — Security techniques — Privacy framework	ISO/IEC 29100:2011 provides a privacy framework which • specifies a common privacy terminology; • defines the actors and their roles in processing personally identifiable information (PII); • describes privacy safeguarding considerations; and • provides references to known privacy principles for information technology.	Status - Is publicly available - https://www.freestandardsdownload.com/iso-iec-29100-2011.html
ISO/IEC 29184: 2020	Online privacy notice and consent		(just published - not available to public - we are working on publishing a report /appendix for use with this group)
W3C DPV 0.01	Data Privacy Vocabulary	• legal ontology for technically breaking down and mapping legal ontology to a data legal ontology - • the Notice + CR V1.2 and W3C DPV, also use a common set of purpose categories. and the Kantara CR v1.1 for purpose specification • (note shared by initial FIHR approach - now much more evolved)	• active - • additional information ◦ Background: EU Funded Project Special ◦ Creating a Vocabulary

Reference: OPN-Notice Schema

OPN: Open Notice (+ Consent) Receipt Schema: Starters Guide to Unified Data Control Schema

Lizar, M. & Pandit, H.J., OPN: Open Notice Receipt Schema, 14th International Conference on Semantic Systems (SEMANTiCS 2019), Karlsruhe, Germany, 2019 [Published http://www.tara.tcd.ie/handle/2262/91576 [accessed July 1, 2020]

Field Name	Field Label	Format	Description	Required /Optional
Schema Version	version	string	The version of specification used to which the receipt conforms. To refer to this version of the specification, the string "v1" or the IRI "https://w3id.org/OPN/v1" should be used.	Required

OPN Privacy Profile URI	profile	string	Link to the controller's profile in the OPN registry.	Required
Type of Notice Receipt	Notice Receipt	string	Label Notice Receipt	Required
Receipt ID	id	string	A unique number for each Notice Receipt. SHOULD use UUID-4 [RFC 4122].	Required
Timestamp	timestamp	integer	Date and time of when the notice was generated and provided. The JSON value MUST be expressed as the number of seconds since 1970-01-01 00:00:00 GMT (Unix epoch).	Required
Signing Key	key	string	The Controller's profile public key. Used to sign notice icons, receipts and policies for higher assurance.	Optional
Language	language	string	Language in which the consent was obtained. MUST use ISO 639-1:2002 [ISO 639] if this field is used. Default is 'EN'.	Optional
Controller Identity	controllerID	string	The identity (legal name) of the controller.	Required
Legal Jurisdiction	jurisdiction	string	The jurisdiction(s) applicable to this notice	Required
Controller Contact	controllerContact	string	Contact name of the Controller. Contact could be a telephone number or an email address or a twitter handle.	Required
Link to Notice	notice	string	Link to the notice the receipt is for	Optional
Link to Policy	policy	string	Link to the policies relevant to this notice e.g. privacy policy active at the time notice was provided	Required
Context	context	string	Method of notice presentation, sign, website pop-up etc	Optional
Receipt Type			The human understandable label for a record or receipt for data processing. This is used to extend the schema with profile for the type of legal processing - and is Used to identify data privacy rights and controls	

OCA schema specification: *https://docs.google.com/spreadsheets/d/1KOdq8Yy3OXmuELyh7tpHMlhyMZPSZ3Ib/edit#gid=68769926*