Controller Credential Specification Overview

(Draft specification in progress)

Process in progress: 1. Updated March 24 2. Notice Controller Credential Specification 3. Papers (in progress) a. Decentralized Data Governance b. identity interoperability	**Notice & Consent Task Force** **Project owner:** Mark Lizar **Editors** Surveillance Controller EditorSalvatore DAgostino Schema Editor:	**Status** ACTIVE
	Notice Controller Credential builds on the Kantara ANCR, Consent Receipt Record format, to provide a digital controller credential,	

Introduction

In privacy regulations and for decentralized identity, transparency is a key requirement. As identifiers are personal, used to track, surveil and profile its not only important to know who controls personal information, but it's required for consent, a critical component of security and a pre-requisite for digital privacy. Most notices, notifications, T&C's don't use standards to provide the transparency over who control's personal information.

This is the focus of the Kantara ANCR Record, which is the prefix to consent receipts.

This controller credential utilizes a reference architecture that began with 1980 OECD Guidelines, and has been worked on for international /internet scalable data governance. This work has driven regulatory reform and convergence internationally. GDPR refer framework for digital.

This controller credential specification extends this international governance standard to the Trust over IP Governance Framework and is used to generate purpose specific micro-credentials for the governance of digital information with SSI's. This enables the use of this reference architecture to scale analogue notice and consent to electronic eNotice and eConsent for digital exchanges and interoperability.

Reference Architecture

- 0PN Transparency WG: Decentralized Data Governance
  - eNotice and eConsent identity & data governance information structure
- ISO/IEC 29100
  - 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.
  - ISO/IEC 29184 Online Privacy Notice & Consent
  - ISO/IEC 27560 WD 5 Consent record information structure
- ISO 27002 Series : WG 5 SC27
  - ISO 27001 sets forth the compliance requirements needed to become certified. In contrast, ISO 27002 is a set of guidelines that are designed to help you introduce and implement ISMS best practices.
- CoE 108+
  - International GDPR -
    - data governance framework which provides the international enforcement policy baseline suitable for internet scale data control, identity transparency governance and consent
- W3C Data Privacy Vocabulary
  - V.5
- Kantara
  - ANCR Notice Record

Specification Overview

This specification builds upon the Kantara ANCR Record specification (and Consent Reciept)(ref) to build a notice controller credential for specifying all of the PII Controller's information in a eNotice record.

The ANCR Record provides Consent Types to anchor a trust record, which the individual owns and controls In a personal data store and profile.

The Record and Receipt specification uses ISO/IEC 29100 Security and Privacy techniques ref (free ISO specification) terms and definitions to identify the legal stakeholders(ref) and their roles in the processing and control of personal information. Using international standards for creation of a regulated data controller credential and for its utility in generating eNotice records and eConsent receipts.

ISO/IEC 29184 - Online Privacy Notice and Consent Controls -

Fields Added to ANCR Record to Create Verifiable Credential

ANCR Record spec - is here (enter link)

This credential is for transparency and accountability for data (and identifier) governance,

The eNotice (PII) Controller Cresdential, is used to generate eNotice record, for micro-credential PII Principal

1. PII Controller Identifier [DiD]
    a. Credential ID
    a. Accountable Person
    b. Accountable Person role
    a. Controller Notice Record Identifier
    a. As a DiD: Verified Credential

1. Controller Type[Ctype]:
    a. Notice Controller,
    b. PII notice controller,
    c. PII controller,
    d. PII surveillance controller , (info not provided by PII Principle)
    e. [Ctype] controller operator,
2. Accountable Person Type

Assessment

ANCR Record provides a PII Controller Digital privacy transparency KPI, be assessing a notice for digital and physical controller identification and privacy access information, as required for the operational use and management of digital identifiers.

The Controller Credential assessment tests this credential for its transparency performance.

Security Considerations

The use of blinding identity taxonomy for personal identifiers includes the Accountable person identifiers, which are required to be published and available in accordance to local legislation.

The identifiers used in the controller credential are specified according to regulation and implemented with standards in order to be subject to regulation and regulatory considerations,

Mitigation Risk

Using standard framework for transparency of control with data control defaults

Examples

1. Security,

Controller Credential

Micro-Credential

defined as a credential specified to a specific purpose.

Glossary

Privacy Stakeholders - ISO 29100

Privacy Stakeholders	ISO Definition	
Regulator /		Privacy Regulator for individuals

PII Principal		
PII Controller		
Joint PII Controller		
PII Processor		
3rd Party		another person, or police,

Annex: Privacy Stakeholder Mapping to Functional ToiP Roles

Continuing of the ANCR Record Assessment to identify the controller credential,

Map the ToiP functional role to the legal authority, justification and role of the stakeholder.

Questions:

Is the controller the holder, verifier, or issuer?

ISO Term	TOIP Terms			
Controller	Holder, verifier, issuer			
Principal				
Processor				
controller contact	extend consent termination for a control point			

Delegated Authority Examples :

			Delegated
Regulator			Ombudsman
PII Principal			Guardian/Parent/School
PII Controller			Joint-Controller
PII Processor			Sub-Processor
3rd Party			turtles

References for Controller Credential, Infrastructure and Legal Framework

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: 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
Notice 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*