ToiP - Controller Credential - (current)

Kantara Initiative Advance Notice and Consent Receipt WG late stage draft.ToIP – DDG: Controller Credential Specification
Version 0.7.1
July 4, 2022
Abstract
This is specification builds upon the Anchored Notice and Consent Receipt (ANCR) Record Specification and its schema to specify a controller credential. Building upon the operational privacy an transparency of the ANCR record to provide a KPI for assessing the performance of the operational privacy and its associated PII Controller security.
This is accomplished by specifying a regulated controller credential from international (non-national) standards and requirements that are reflected in laws and regulations. The Controller Credentia can then be it's holder to specify and negotiate the delegation of authority of data control and governance amongst all privacy stakeholders. This establishes the basis for standardized digital identifier governance utilising evidence of Consent to decentralized the control of personal data and it's processing.
The ANCR Record Semantic Schema Stack:

- ISO/IEC 29100 Privacy and Security techniques framework
- CoE 108+ International legal framework
- Kantara: ANCR Record
    - See ISO/IEC 27560 Consent record information structure
    - See ISO/IEC 27561 Privacy operationalisation model and method for engineering (POMME)
- Kantara: Consent Receipt v1.1
    - See ISO/IEC 29184 Online privacy notices and consent
- OCA
- Kantara Blinding Identity Taxonomy
- W3C Data Privacy Vocabulary DPV

 h1.Foreword

This specification is developed in conjunction with an ongoing body of work that includes a stack of other specification efforts, which in term are incorporated into the development of standards, and a co-regulation framework presented here in a eNotice code of conduct, and eConsent code of Practice for accountability and consent with transparency.
The scope of this specification is to define a controller credential for ToIP along with a global decentralized data governance framework. The framework shows how to enhance the performance of transparency and accountability, and at the same time decentralized control of identifiers to identity management systems, where often control or out of scope of defined in bespoke asymmetric policy..
The overarching decentralized data governance framework is steered from the 0PN: Public Benefit Consortium committed to engineering digital privacy for people and enable provide, up until now, elusive, digital trust for SSI.
This publicly available <guide, template, spreadsheet, etc.> was approved by the OPN Steering Committee and the ToIP Foundation Steering Committee on [date of approval (dd month yyyy)].
The mission of the Zero Public Network (0PN) is to define a complete architecture for digital privacy and decentralized digital identifier governance where effectively zero exists today In some sense this is a Zero Trust Architecture from a human risk perspective. Another reason for creating Zero Public Network.. The 0PN Decentralized Data Governance framework v1.X utilizes international (non-national) standards, legal frameworks and the AuthC Authorization from Consent (AuthC) is the term given to the human centric access control protocol as it requires knowledge, understanding, and control over data activity before consent to any further activity takes place. protocol for eNotice and eConsent. This framework is mapped here to the ToiP – Digital Trust / Security Architecture?t?? to support decentralized data governance in support of the ToiP Governance Framework.
The mission of the Trust over IP (ToIP) Foundation is to define a complete architecture for Internet-scale digital trust that combines cryptographic assurance at the machine layer with human accountability at the business, legal, and social layers. Founded in May 2020 as a non-profit hosted by the Linux Foundation, the ToIP Foundation has over 300 organizational and 100 individual members from around the world.
Note: Human Colossus IPR?Note: Human Colossus IPR?
@paul
Please see the end page for licensing information and how to get involved with 0PN and the Trust Over IP Foundation.<ac:structured-macro ac:name="anchor" ac:schema-version="1" ac:macro-id="cc95149e-70e0-438a-844c-67ef148cdc45"><ac:parameter ac:name="_heading">h.2s8eyo1</ac:parameter></ac:structured-macro>

Introduction

Digital Identity Security

Document

To Address a critical security flaw native to digital identity technology, where people are a) identified before the authority to generate an identifier or process personal data has been granted b) are unable to see which PII Controllers are processing personal data and when they are processing it after it is collected.
Critical Security Flaw – notice to digital identity technology is the lack of notice or standardized transparency over who is control, prior to authentication, lack of mutual agreements on authorization,

- - ***no transparency over authority to process up front,***
  - ***No transparency over controller, and controller privacy risk***
  - ***Not transparency over the service privacy risk -***
    - ***Disclosure of identifiers without transparency***
- ***SSI Governance***
  - ***Without decentralized transparency DiD's can only be distributed***
  - ***Requires international and internet saleable data governance framework***
  - ***Requires data governance to scale in identity systems***

The 3 goals of this specification are to;

- ***Specify data control credential fields to embed digital transparency to address the critical security flaw .***
  - ***DiD- Serialization – Record as a container – the log file of its useage – Kerri Receipts***
- ***Specify and assess the performance of transparency and access to controller credental –in terms *data controls specified 2nd KPI***
  - ***Credential Performance KPI – at a certain performance leve = DDE***
- ***Specify how to map digital transparency to ToiP Framework***
  - ***Semantics, roles, (tech eat culture vs culture eat tech)***
    - ***Governance to Governance***
    1. ***Trust to Trust***
  1. ***Internatioanl authoritative law for PII Principal***
     a. ***Table***
     b. ***Trust = this***
     c. ***Governacne***

Document ***Information***

ToiP ISWG Project : Notice and Consent Task Force

Contributors

- Mark Lizar – Author
- Sal D'Agostino - Editor

Acknowledgements

- Global Privacy Rights NGO - Zero Public Network (0PN) Public Benefit Consortium
- Human Colossus
- ANCR WG
- W3C Data Privacy Vocabulary
- IS0/IEC 27561

IP

Revision History

Version	Date Approved	Revisions
1.0	DD MONTH YYYY	Initial Publication

Terms of Use

Language and Terminology

The following conventions SHALL be used in this document:

1. Words and abbreviations that are in **bold** font have a specific meaning in this document and are defined in the appended / linked Glossary. All terms and patterns or mental models used in this document SHALL be defined in the Glossary, a **controlled document** of the 0PN: Decentralized Governance Framework, which utilizes
2. The GF SHOULD be written in plain language.
3. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119
4. Only one **governance framework** document will be created, where policies, rules or controlled documents apply to lower layers of the ToIP stack, they SHOULD be tagged #LayerX.

Normative References

1. ANCR Record V.0.9
2. ISO/IEC 29100 *Security and Privacy Techniques framework*

This international standard provides a mutually exclusive and collectively exhaustive security and privacy stakeholder specification and has been used to guide the development of international data governance for transborder flows of perosnal data

1. normative CoE 108+ legal framework to baseline performance of the data control and credentials which may have multiple ToiP roles.
2. Normative ISO/IEC 29184 - Online Privacy Notice and Control

Non-Normative

1. Non-Normative W3C Data Privacy Vocabulary for notice, notification and disclosure
2. Non-Normative 27560 – Consent Receipt standard for record
3. Blinding Identity Taxonomy

Referential

ISO/IEC 29115:2013

This standard provides a framework for managing entity authentication assurance in a given context. In particular, it:
specifies four levels of entity authentication assurance;
specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance;
provides guidance for mapping other authentication assurance schemes to the four levels of assurance (LoAs);
provides guidance for exchanging the results of authentication that are based on the four LoAs; and
provides guidance concerning controls that should be used to mitigate authentication threats.

Terms and Definitions

Terms and definition presented here are in reference to the controller credential fields and their definitions which are in addition to the Kantara ANCR-Record specification.

Accountable Person

Controller Credential

Controller Type

Electronic Consent (eConsent)

Electonic Notice (eNotice)

PII Notice Controller

PII Controller Operator

PII Controller (Governance) Registrar

Micro-Controller Credential – ANCR Record + fields (secure not accessible raw data, must

Verified Micro-Credentials

Micro-Consent Receipt Token

Signing protocol for the parties

Controller Credential Fields

1. Regulated Credential
    a. Transparency has always been required but largely ignored in contract-based governance models, like terms and conditions or end user licenses.
    b. Builds in security and privacy, used for any type of notice
    c. digital twin of PII Controller fields from anchor receipt
        i. credential of the controller, use for mitigating risks and generating micro-credentials
            1. public controller credential can be assured in many ways, {color}
               #### Providence of controller authority
            2. Providence of accountable person authority

ii. The authority of the credential –

2. Builds in security and privacy, used for any type of notice
3. digital twin of PII Controller fields from anchor receipt
    a. credential of the controller, use for mitigating risks and generating micro-credentials
        i. public controller credential can be assured in many ways, {color}
        ### Providence of controller authority
        ii. Providence of accountable person authority
    b. The authority of the credential –

o The controller credential can then be enhanced with the role of support person, or an accountable person, and the scope of providence for the credential.

Controller Credential Fields

Fields added to ANCR record schema are controller credential fields that are required for operational privacy and transparency. The controller credential is intended to be linked to any notice or evironemnt where data is being collected, used and processed.

Name of Field	Label	Description			Drafted by
Controller ID					

- Record Identifier
- Controller Company Authority
- Controller Type
- Controller Providence: Local, Regional, National, International
- Accountable Person: Role
- Accountable Person : Delegated Role
- binding the Controller with a Accountable person
o mapping the international data governance framework to ToiP functional trust model
o Issuer Hold
Transparency over the performance of Data Controller Credential in ToiP governed DiD's

This fields are added to the ANCR record to provide the missing digital trust governance fields to a Controller Credential Fields. Fields specified here are added to the ANCR Notice Record,

1. Accountable Person and role
2. Controller Receipt Identifier

3. Rpbert

- PII Controller Credential Identifier [DiD]

- Serialization
- linking
4. - Paul - bliding identity taxonomy – Rule set – specified and implement. - requirements
– PII Principal – contorls the record – must provide eCosnet to give access, share, - transparency over 3rd party dicslousure and use -
- usable automatically – for generatingVS – for a micro-credential
- accoutanble -
2.1 Verified Credential
- Robert
3.

Controller Type[Ctype]:

- Mark
b. PII notice controller,
c. PII controller,
d. PII controller operator

Controller Identifier

Their are 3 identifiers and corresponding key pairs specified for this specification.

1. The Controller Credential ID / DiD
2. it's use and serialization
3. Blinding Identity
4. The Use with OCA in regards to identifiers
5. Security of Identifiers
6. Generation of a Micro Credential
7. Generation of
8. The ANCR 'Anchor Notice Record iD' link to hash of the text which text copy,. Proof of Notice -
    a. Two Factor Notice for Proof Of notice
    b. which is anchored to the PII Controller Notice and the PII Principal's capture of the notice (or equivalent)
9. The consent notice receipt iD that is generated when a PII Principle interacts with the notice, context of a sign or notification
10. operation of these fields
11. accountable person is a blinded identifier field
12. legal entity officer, unless delegated

Operation of Credential

Mapping to ToiP Governance Architecture

Semantics

Operational Privacy Transparency

Embedding Credential and linked Profile

Operational Privacy Performance KPI

1. a. The ANCR Operational Privacy Transparency
        i. Key Performance Indicator

Data Control, Exchange and Access

Generating a micro-credential that is verifiable

1. a. From Embedded PII Controller Credential
    b. Self Asserted (PII Principle) Asserts a Verifiable Credential and a 3rd Party Notary

Exchange of eConsent Tokens:

1. a. Used for exchange of micro-credentials Outside of the Data Store, or Data Store Control Interface e.g. Digital Credential Wallet,
        i. Note: TDAOperational Privacy Transparency
2. ANCR Schema for
    a. Electronic Notice : ANCR Record Part 2: Purpose Specification Once specified, an eNotice can be generated
    b. Part 3, utilizing the Data Privacy Vocabulary
    c. Part 4 with reference to specific regulation and or a code of conduct , along with any certified codes of practice

Scalability

Overlay Capture Architecture

a. OCA is used to map and overlay the field name and label of the corresponding legal privacy elements, and to assess conformance of the credential information against standards, laws, and codes of conduct and codes of practice
iii.Regulated Credential Mapping
1. any stakeholder can create a controller credential, making it ideal to provide as a public utility for transparency conformance with regulation for health, safety, data disclosure, sharing, monitoring, and as permission transport vehicle in the form of a token.
a. a controller credential can be used to generate micro-credentials by signing concentric notice receipts that are generated from an ANCR Notice Record.

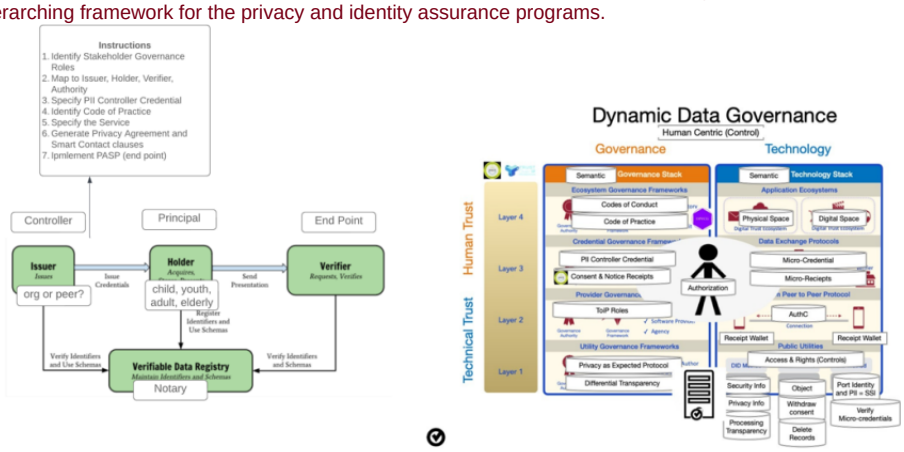
Security Considerations

The 0PN Decentralized Data Governance framework employs a Data Control Impact Assessment (DCIA) in order to make transparent the control and trust vectors for a specific system and service.
The Controller Credential is embedded into notices, notifications and disclosures to address self-soverign transparency requirements for decentralized data governance. This embeds the missing security for personal data control in a notice or notification.
This provides the transparency discovery mechanism for the individual to provide the authority to generate and processes a decentralized identifier.
In this way, this specification will address native security flaw in native to digital identity management systems which in effect governance of this alpha surveillance technology.
Achieving Objective 1 of this specification for a ToiP standard.
More information, The credential, and use of DiD's for verifiable credentialling is addressed in the 0PN Decentralized Data Governance – trustworthy Identity system architecture. (ref)
credential with lack of standard transparency over Authority, e.g. who a person is consenting too and what
The DCIA – provides this standardized transparency over the scope of authority and the providence of the decentralized Identifier, in order to :
1. a) create and manage digital identifier
2. b) to process and permission personal information
iii.the controller credential provides a public credential for people to more easily and use for its intended purpose, which is transparency over who is accountable
iv.the person acting on behalf of the company, as well as the accountable person safeguarding the company are roles that are regulated, providing a regulatory framework and tools set for the governance of SSI

1. Blinding Identity Taxonomy is used to blind the PII Principals identifiers

ToiP Governance Interoperability

Mapping Governance
Key is mapping the authoritative and international standards to the ToiP gov model.
Semantics
First are the semantics, table of the different terms that are used then mapped to the ToiP framework,
Second, is the DCIA
Third is the stakeholder roles from DDG to the functional roles in the ToiP stack, e.g. holder, verifier etc. These provide governance authorities with an overarching framework for the privacy and identity assurance programs.



Governance Semantics

i.the international privacy frameworks which are represented with a privacy controller credential provide a human centric definition for some terms which differ from ToiP's, functional identifier centric glossary,
a. Identity,
b. Permission
c. Governance
d. Trust
e. DGA Registry: culture and privacy regulations are rich with these standard terms and definitions which have evolved since the 1980 Transborder flows of personal data, from best practice, to standard, to regulation, and with CoE 108 +, an international framework for robust data governance.

conformance assessment of ToiP framework

When reviewing an SSI system, First define the service point and context of identifier use. In this context identify which SSI stakeholder is the PII Controller.
1. Is it the verifier, the issuer or the holder?
2. Factors of Authority & Delegation
1. First Factor Policy: Apply legal governance rules according to the location of the PII Principle
2. Second Factor Policy: Apply contract governance rules
3. Terms
a. First Factor Policy (regulatory)
PII Principle Policy – interacting with a public (relevant to all stakeholders)
Big G – Gov – for physical and public space.
1. implementing law with codes of conduct which are used to extend regulation for a specific sector, industry, context. Reviewed and approved by a regulator.
b. Second Factor Policy (co-regulatory)
i.Parental Consent, Terms and Conditions, by laws, representing local, context specific or regional policy
c. Third Factor Policy i.ToiP Stack
d. Fourth Factor

- Micro Ledgers
  receipts

Appendices for General Governance Requirements

The Trust Over IP Foundation (ToIP) is hosted by the Linux Foundation under its Joint Development Foundation legal structure. We produce a wide range of tools and deliverables organized into five categories:

- Specifications to be implemented in code
- Recommendations to be followed in practice
- Guides to be executed in operation
- White Papers to assist in decision making
- Glossaries to be incorporated in other documents

ToIP is a membership organization with three classes—Contributor, General, and Steering.
The work of the Foundation all takes place in Working Groups, within which there are Task Forces self-organized around specific interests. All ToIP members regardless of membership class may participate in all ToIP Working Groups and Task Forces.
When you join ToIP, you are joining a community of individuals and organizations committed to solving the toughest technical and human centric problems of digital trust. Your involvement will shape the future of how trust is managed across the Internet, in commerce, and throughout our digital lives. The benefits of joining our collaborative community are that together we can tackle issues that no single organization, governmental jurisdiction, or project ecosystem can solve by themselves. The results are lower costs for security, privacy, and compliance; dramatically improved customer experience, accelerated digital transformation, and simplified cross-system integration.
To learn more about the Trust Over IP Foundation please visit our website, https://trustoverip.org.