ANCR WG ISO/IEC JTC1 WG5 ANCR Transparency Performance Scheme Contribution Deep Dive

(ANCR WG Contribution & Report for ISO/IEC wrt submitted comments to ISO/IEC 27091, 27566, 27568)

April 6, 2024

Contents

1. Liaison Contribution

This contribution has multiple purposes:

1. A liaison contribution from Kantara to ISO/IEC JTC1 WG5 to facilitate forward progress on an international digital privacy transparency trust assurance program.
2. To provide a benchmark for regulatory oversight for an authority-based authentication and authorisation framework (not based on NIST LOA's). This new notarial assurance framework is characterised by the surveillance of the Controller Identity, whose identifiers are used as a proxy to identify the individual when required. Privacy-centric authentication provides people with ability to access digital privacy rights without having to first give up privacy to access rights, this enables digital privacy at scale utilizing dynamic levels of transparency and verifiable assurance. This is opposed to current digital identity-centric frameworks, which first identify the individual, requires the transfer of raw personal data across the internet and thus perpetuates an insecure data protection, rather than co-regulatory privacy model.
3. Benefits of Digital Privacy, designed to address Digital Privacy's inherent security and privacy gaps.
    - Consent notice receipts provide proof of notice and knowledge, provide for anonymous real consent with a break the glass dynamic data access for security services, but does not require passwords or the transfer of PII over the internet directly. It enables personalised privacy, private and secure AI and addresses misinformation.
4. To inform a joint relationship management plan for a proposed international assurance program:
    a. Industry collaboration between physical security industry represented by Sal D'Agostino (and SIA)
    b. A data privacy officer certification program for Controller Notary Credentialing. represented by Sharon Polsky, President of Privacy and Access Council of Canada.
    c. A Kantara initiative, Framework Registry of Registrars. This would facilitate international digital consent governance, enabling dynamic cross-border security, cross-border policing and emergency service access to PII, in accordance with Convention 108+.
5. To introduce a Transparency Trust Assurance Levels and a Registry of Registrars for digital consent across jurisdictions, in compliance with the Commonwealth legal Convention 108+

2. Introduction

These inputs into JTC1 WG 5 inputs from Kantara initiative ANCR (Anchored Notice and Consent Receipt) WG apply to the use of ISO/IEC 29100 framework. They are applied natively in the context of conformance with 29184 Online privacy notice and consent and the Kantara Consent Receipt, also represented in the consent record information structure ISO/IEC 27560. Although it is applied as the Notice Record information structure to enable consented information structure.

As the authors of the Kantara Consent Receipt contributions to ISO/IEC JTC 1 WG5 27560, the ANCR WG has developed not only the Consent Receipt, but also a conformance and compliance assessment framework, called the ANCR Transparency Performance Scheme (TPS).

This Scheme is designed to be expansive, applied to ISO/IEC that measure the conformance to these standards and the compliance of Controller Identity records, with Convention 108+ and GDPR's Chapter 1, transparency modalities.

3. Transparency Performance Scheme Applied

The TPS is applied to make security and privacy risks operationally transparent in the use of digital identity management for all stakeholders across physical and digital spaces. This is regardless of the legal justification, i.e. whether the primary purpose is consent or not.

Beyond its regulatory applications, the ANCR Scheme provides the framework for benchmarking the assurance provided by TPS based schemes. It is currently part of a proposal for a Kantara Initiative Transparency Trust Assurance Scheme for digital identity credentials proposing a Registry of Registrars, a registry of international controller registrars. This would enable dynamic consent and international data access between jurisdictions and borders.

The ANCR TPS, for Conformance and Compliance measures compliance by first generating a conformant Controller Record in accordance with 27560 Consent record information structure (to ANCR record TPS framework). The record, also referred to as a PII Controller Credential, can natively be assessed against ISO/IEC29184 Online privacy notice and consent standard, as well as privacy laws, like the GDPR (mirrored in Convention108+). The independent record is then utilised to measure the operational performance of notice, measuring how open, transparent, complete, and dynamically usable notice, notification or disclosure are to the individual.

4. Using the Scheme

The ANCR WG and its predecessor continue to be long-term contributors to ISO SC 27 WG5. The ANCR TPS builds directly on these contributions, providing a tool for regulators to benchmark security and privacy of identity management systems by generating a Controller Notice Record, that enables active regulatory auditing and assessment, and the scaling of data governance online.

Digital transparency refers to the creation of standard record and its mirrored consent receipt for any notice, notifications and disclosures using the same record format. Digital Privacy requires a record for all data processing in accordance with Article 31 Records of Processing Activities, and Article 80 of Convention 108+.

Digital privacy transparency is the cornerstone of personal security, as it not only enables stakeholders in data processing to see and understand security and privacy risks but also who is liable applying transparency scheme using a single standard.

5. The TPS in its Initial Draft as a Two Part Scheme

Part One consists of four Transparency Performance Indicators (TPI) used to generate the controller notice record in the conformant record format for transparency and consent (27560). Significantly, the TPIs listed are used to measure how dynamic the performance of transparency is, unlike any other measure or assessment.

Part Two, within the appendix of the TPS scheme, provides the steps to use the Controller Notice Record to administer personal data using a standard set of consent-based rights used to control the processing of personal data. Note: in Quebec

6. Transparency Performance Indicators (TPI) Explained

TPI 1: Measures whether the PII Controller information is provided prior to data capture, just in time, at the time of data capture, or after data is collected and processed. The Controller identity, governance and accountability information is captured in the record on this first TPI

TPI 2: Measures the completeness of the Controller information. Currently, with all digital services, there is not enough Controller Transparency in context for individuals to use rights to control their data. People are isolated under terms and conditions online.

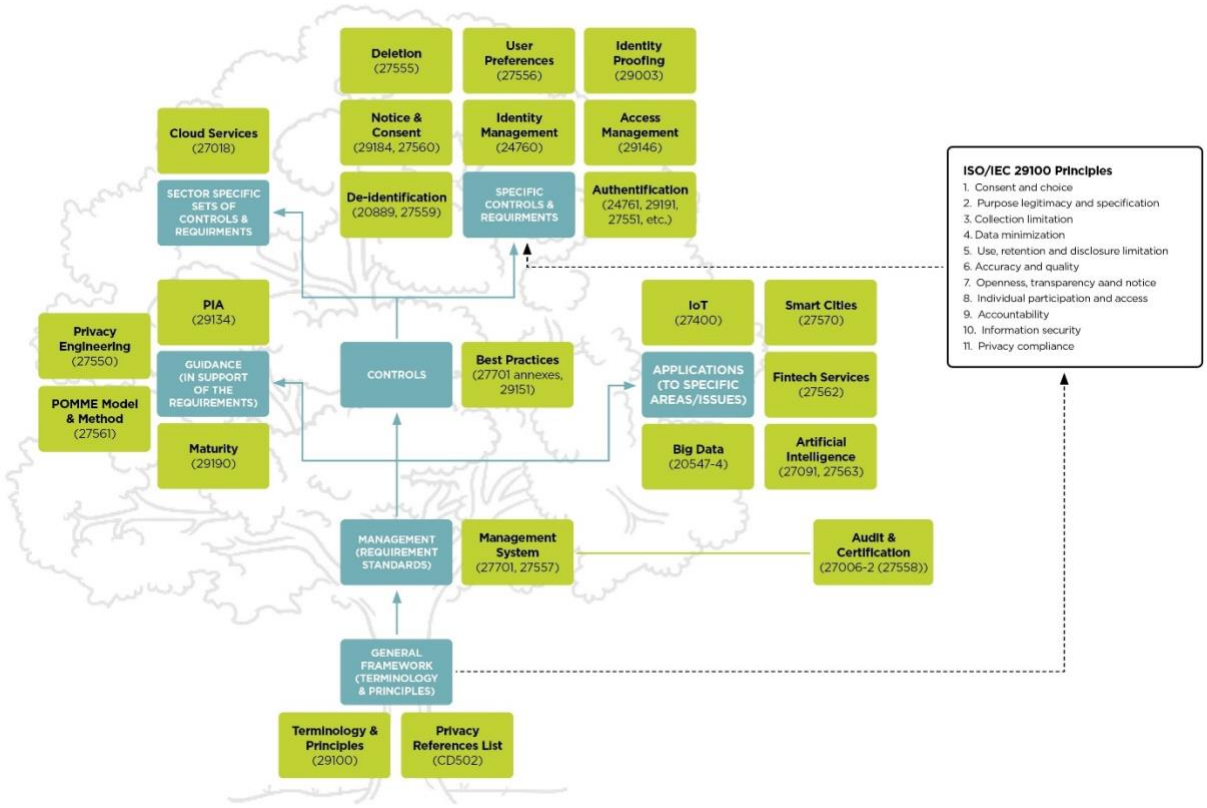
TPI 3: Measures the accessibility of controller notice credential information. This TPI assess how dynamically assessable the controller information is in a digital service context. This captures if the individual needs to scroll a page view, click a link etc. to use

the security and privacy information to control data processing in context. This provides a measure of the contextual integrity of Controller Transparency and Accountability.

TPI 4: Measures certificate and/or Token information performance indicators. The TPIs are attuned to the location of the PII Controller, and the scope of PII disclosure. This TPI captures if the country of the PII Controller match the certifications, if there is a third party jurisdiction involved, which personal data, or micro-data, is transferred in processing (treated as meta-data), and this can be indicated in the SSL certificate. In this assessment, the security, surveillance and privacy risks can be assessed by examining the PII Controller Notice Record to see if the required (knowledge) notice, notification or disclosure was provided to the individual.

7. Status of the ANCR Transparency Performance Scheme

The Transparency Performance Scheme (TPS) is nearing its first final draft. We are looking to advance this specification in line with the 27566-2 Age Assurance benchmarking standard,in order to be applicable to the suite of security and privacy standards for identity management related technologies and schemes. The suite of specifications interoperable with the 29100 security and privacy framework, shown in the diagram below, provide a roadmap for the development of this scheme to enable standard protocols for creating records of processing activities for active regulatory oversight, and the mirrored consent receipt record, to digitally twin privacy and security.



ANCR TPS prioritises 29100 principle 7, Openness, Transparency, and Notice, elevating this to principle #1. Consent and choice are thus moved to principle #2, as operationally, the quality of consent and the subsequent choices for permission, access and processing of personal data first requires proof of knowledge, which is a core metric of the TPS. As of March 7 2024 , when the DSA/DMA came fully into force, functional digital transparency for legitimate consent is clear requirement. This is why a notice record for proof of notice/knowledge is required to address this non-compliance at scale, which is supported by the recent EU court of justice ruling on the IAB transparency and consent framework (March 8 2024). Without functional digital transparency, and a record of it for all parties, it is not operationally, legally, or humanly possible to provide valid consent, that is, to have a valid choice. This equates to a non-compliant implementation of a digital identifier surveillance technology.

8. Conclusion

The standards that the ANCR WG has been applying the ANCR work to, with comments, follows. We will be adding further standard case studies in due course.

1. Consent Receipt
2. Transparency performance -Security Scheme

3. Controller Notice Credential – uses the PII Controller 27560/Consent receipt purpose specification, and record structure, focusing on Notice Records and the use of this record for generation of consent tokens by the PII Principal.

We would like to continue to work through the liaison between Kantara and ISO. We look forward to engaging further the security, privacy and identity industries with this new transparency and trust framework to enables real human consent online.

Thank you for the opportunity to participate.

Appendix A: ANCR WG Contributions

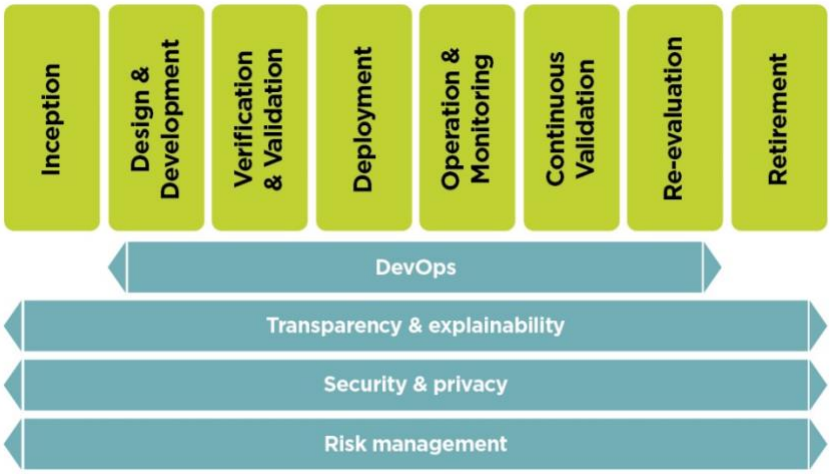
The ANCR WG has submitted, through the Kantara Initiative liaison, comments introducing this scheme to:

1. 27561: Security and privacy in digital twin. Please note that we mean this in the sense of how to twin digital security and privacy, while the standard is instead focussed on the security and privacy of a digital twin. Our focus was on how to mirror these records to enable transparency for humans from digital twinning specifications in this capacity and apply it to other standards.
    - This first round input, which is in the process of being updated in line with this document, can be found on the ANCR wiki. ANCR-27566 input to SC 27, WG5.
2. 27566-1: Age Assurance (referred to as Age Surveillance in ANCR scheme). ANCR WG submitted comments requiring a consent receipt for its use to be provided to the individual. Or, when for legal and security reasons, transparency is deprecated, a consent receipt is provided to the governing regulator. This enables compliance with Canadian transparency and consent laws, specifically, Quebec Law 25, in which an individual can provide a secondary purpose for consent, regardless of the legal justification for processing.
3. 27091: Generative AI privacy and security
    - The TPS is easily extended to Generative AI, to first measure whether or not the information in a Large Language Model (LLM) is captured with consent
    - In the ANCR TPS for Generative AI, legitimate PII processing requires a record of activity. This can be achieved by providing the individual with a consent receipt for any first engagement with a Generative AI service, linked to a log of any subsequent uses of that AI. This enables individuals to query AI and

track the processing of their personal data by AI, which enables co-regulation of AI by all privacy stakeholders.

Appendix B: Assessing Transparency Performance of Generative AI

In 27019, the following lifecycle and layers are presented:



This diagram illustrates applicability for security and privacy operational risks measured by and benchmarked with the TPS.

- DevOps is the operational context within which the security and privacy risk to required transparency are measured. The PII Controller in this case would receive a credential for this identity and access management service.
- Transparency and explain ability are captured with Transparency Performance Indicators. Visual signals represent a new transparency modality, where the transparency conformance and compliance of a controller record can be presented visually without the need to read additional policy or notice.

The ANCR Scheme can be applied to provide assurance for the compliance, trustworthiness. and reliability not only of PII Processing, but also the information linked to a PII Controller. This addresses mis-information security for those systems that deploy TPS based assurance because the Controller is identified from the outset and therefore the information that is shared can be held accountable by all stakeholders. This is applicable from:

- Inception

    - This is the initial notice and receipt used by the PII Principal to capture the security and privacy state.
- Design and Development
    - Based on the notice, the fields and details in a PII Controller Notice Record, can be used as a Credential to generate notice records and consent receipts, independently of the PII Controller.
    - The scheme focuses on the assurance and security of the controller records, not assurance of the individual's digital identity or verified credential. This transparency enables authentic consent
- Verification and Validation
    - The details of the PII Controller Credential can then be verified and validated for each of the TPIs
        - Timing of the Notice
        - Content of the Notice
        - Usability and Accessibility of the Notice
        - Security Coherent with the Notice
- Security and Privacy
    - The TPIs measure the security and privacy provided in the notice for the information and performance verified and validated.
- Risk Management
    - The record created provides and maintains a Record of Processing Activity (RoPA) that is made available to all parties, so that there is a common risk framework and understanding.
- Governance
    - The TPS and its TPIs provide a means of ***co-regulation***, making it possible for the PII Principal, the PII Controller and regulators to effectively engage in decentralized, distributed and internationally interoperable data governance, assurance contextual integrity for high-risk security and privacy contexts, and assuring this integrity through dynamic data controls.