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

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



April 4, 2022

## Purpose of Input to Kantara LC and Board

This input has multiple purposes:

1. This is a Kantara liaison contribution from Kantara to ISO/IEC JTC1 WG5.
2. This input is intended to facilitate forward progress on an international digital privacy transparency trust assurance program.
3. This contribution aims to provide a benchmark for regulatory oversight for a different Authentication Assurance Scheme that focuses on the identification of the binding of the controller notice record and Controller Notarial Credential that enables;
	1. Proof of notice, anonymous real consent, with a break the glass dynamic data access for security services, does not require passwords, or require the transfer of PII over the internet directly. enables personalised privacy, private and secure AI, address misinformation at scale. In effect address security and privacy gaps with Digital Privacy.
4. This input informs a joint relationship management plan for this proposed international assurance program,
	1. Planning for an industry collaboration between physical security industry represented by Sal D’Agostino (and SIA)
	2. A planned data privacy officer certification program for Controller Notary Credentialing. represented by Sharon Polsky, President of Privacy and Access Council of Canada.
	3. A proposed Kantara Initiative, Framework Registry of Registrars, to facilitate international digital consent governance enabling dynamic cross border security to break the glass access, cross-border policing and emergency service access to PII, in accordance with Convention 108+.
5. Provide Kantara LC and Board, the background information to better introduce this proposed Kantara Assurance Registry of Registrars Assurance program for digital consent across jurisdictions, in compliance with the Commonwealth legal Convention 108+

## Introduction

These JTC1 WG 5 inputs from Kantara initiative ANCR WG apply to the use of ISO/IEC 29100 framework and is 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 and a contributor to the 27560, the ANCR WG has developed not only the Consent Receipt, conformance and compliance assessment framework, called the [ANCR Transparency Performance Scheme (TPS).](https://kantara.atlassian.net/wiki/spaces/WA/pages/301564731/ANCR%2BTransparency%2BTrust%2BPerformance%2BAssessment%2BScheme)

This Scheme is designed to be expansive, applied to ISO/IEC that measure the conformance to these standards but also, the compliance the of the Notice record with Convention 108+, and GDPR, Chapter 1, transparency modalities.

## TPS Transparency Performance Scheme Applied

The ANCR (Anchored Notice and Consent Receipt) is designed to enable international regulatory assurance for transparency and consent. The TPS is applied to make security and privacy risks in the use of digital identity management for all stakeholders across physical and digital spaces. Regardless of the legal justification, meaning whether the primary purpose is consent, or not.

Beyond its regulatory uses, the ANCR Scheme provides the framework for benchmarking the assurance provided by TPS based schemes and is currently a part of a proposal for Kantara Initiative Trust Assurance Scheme for international controller registrar, registry. Enabling dynamic consent and international data access across borders.

The ANCR Transparency Performance Scheme, for Conformance and Compliance is used to measure 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, is then assessed against 29184 Online privacy notice and consent standard, as well as the legal requirements found in regulation 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 a disclosure are to the individual.

## Using the Scheme

 As such, digital transparency is the cornerstone of personal security, enabling stakeholders in data processing to see and understand security and privacy risks and who is liable applying the transparency scheme using a single standard.

Digital transparency refers to the creation of standard record and consent receipt for of processing activity for all notice, notifications and disclosures with regard to PII processing, and a record (log) using the same record format for all transnational processing of data in accordance with Article 80 of Convention 108+.

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

## The TPS, in its initial draft as a [2 Part Scheme;](https://kantara.atlassian.net/wiki/spaces/WA/pages/301564731/ANCR%2BTransparency%2BTrust%2BPerformance%2BAssessment%2BScheme)

Part 1 consists of 4 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 2, in the appendix of the TPS scheme, provides the steps to use the Controller Notice Record to administrate personal data using a standard set of consent-based rights used to control the processing of personal data. Note: in Quebec

## Transparency Performance Indicators 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: Measure the completeness of the Controller information is. As it is often the case that there is not enough Controller Transparency in context for individuals to use rights to secure themselves according to the perceived risk to the individual.

TPI 3: 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 need to scroll a page view, click a link, or similar 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: Certificate and/or Token information performance indicators. The TPI’s are attuned to the location of the PII Controller, and the scope of PII disclosure. Capturing if the country of the PII Controller match the certifications, if there is a 3rd party jurisdiction involved, in which personal data, or micro-data, is transferred in processing, (treated as meta-data), 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.

## Status of the ANCR Transparency Performance Scheme

The Transparency Performance Scheme (TPS) is nearing its first final draft, and we are looking to advance this specification in line with the 27566-2 Age Assurance benchmarking standard. The aim is to advance this scheme 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 can be seen below in this tree diagram provide a roadmap for the development of this scheme to enable standard protocols for creating records of processing activities for regulatory, oversight, and the mirrored consent receipt record, to digitally twin privacy and security.



ANCR TPS, fundamentally prioritises 29100 principle 7, Openness, Transparency, and Notice, elevating this to principle #1 in this scheme to operationalise this principle. Thus, moving consent and choice to principle #2, as operationally, the quality of consent and the subsequent choices for permission access and processing of personal data requires first proof of knowledge, which is a core metric of the TPS. Fundamentally, as of March 7th, with Digital Services Act coming into force, this clearly required, and without functional digital transparency, and a record of it for all parties, it is not operationally, legally, or humanly possible to provide valid consent, ergo, have a valid choice, and as a result, a non-compliant implementation of a digital identifier surveillance technology.

## Current State of ANCR TPS Contributions

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

1. 27561: Security and privacy in Digital twin with comments, on how to use ANCR Record and Receipt specifications to capture instead the security and privacy of a digital twin, to assess its conformance, compliance and performance.
	1. This first round input, 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.](https://kantara.atlassian.net/wiki/x/GQB4G)
2. 27566-1: Age Assurance, (referred to as Age Surveillance in ANCR scheme) ANCR WG, submitted comments requiring a consent receipt be required 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
	1. The TPS is easily extended to gen AI, to first measure whether or not the information in an LLM is captured with consent,
	2. In the ANCR TPS for gen AI– legitimate PII processing requires a record of the processing activity, this can be achieved by providing the individual with a consent receipt for any first engagement with a gen AI service, linked to a log, of any subsequent uses of that AI. This enables the individuals to query AI, for the use of the PII, and or the PII Principals’ IP, so that this can be governed by individuals themselves.

## ANCR WG Specifications

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 then – the use of this record for generations by the PII Principal

For example, in 27019 the following lifecycle and layers are presented:



This diagram illustrates Applicability for security and privacy operational risks measured and benchmark with the TPS,

* DevOps is the operational context in which the security and privacy risk with regards 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 and with visual signal the transparency conformance and compliance of a controller record can be visually transparency without the need to read additional policy or notice.

## Conclusion

The ANCR Scheme can be applied to provide assurance for the compliance, trustworthiness and reliability of not only PII Processing, but of the information linked to a PII Controller and as a result, address mis-information security for those systems that deploy TPS based assurance, applicable from,

* Inception
	+ This is the initial notice and receipt that is used by the PII Principal to capture the security and privacy state.
* Design and Development
	+ Based on the notice the fields and details a PII Controller Notice Record, can then be utilised as a Credential that is used to generate notice records and consent receipts, independently of the PII Controller.
	+ The scheme focuses on the assurance and security of the controller records, rather than focusing on 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 Transparency Performance Indicators (TPIs)
		- Timing of the Notice
		- Content of the Notice
		- Usability and Accessibility of 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 of 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.

# Appendix: Active TPS Market Applications

## 0PN Data Commons Community Interest Security Architecture Project.

The Digital Transparency Lab (DTLab) is the official incubation lab for the ANCR: Digital Privacy Transparency and Consent Mirrored Record Framework.

This framework represents a collaboration between the physical security, privacy and digital identity industries to create a Digital Privacy Centric internationally regulated transparency and consent framework, to replace the non-compliant ‘I Agree’ contract-based privacy policy framework.

Different Assurance Framework than NIST LOA’s

Controllers Credentials in this framework are used to provide the data subject with Controller based identifiers, rather than PII Principle based identifiers, in this way raw PII is never exchanged over the internet. Individuals can access services anonymously with higher assurance, effectively.

WHiSSPR-Reports

The DTLab, operates a digital identity technology service assessment called WHiSSPR, which stands for **White Hat, identity, Surveillance, Privacy Risk Report**. This identifier/credential centric assessment, assess the risk the individual to focus on provide assurance for PII Principle’s security and privacy,

The WG Co-Chair and TPS Editor, Mark Lizar, is President of the Digital Transparency lab, and works to innovate the TPS assessment, to develop a commercial benchmarking framework called a Transparency Index.

The 0PN Digital Transparency Lab has applied TPS based WHiSSPr-report to assess Canadian proposed privacy legislation Bill [C27](https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c27_1.html#:~:text=Overview-,Bill%20C%2D27%2C%20An%20Act%20to%20enact%20the%20Consumer%20Privacy,Digital%20Charter%20Implementation%20Act%2C%202022.) “An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts” directly related to the standard drafts referenced here as well as to other ISO standards.

In addition, an international assessment of privacy regulations conformance and compliance, applied to Bill C27 in this report. You can find the report linked to the [0PN WHiSSPR Newslette](https://www.transparencylab.ca/s/0PN-DTL-newsletter-Issue-1-Feb-24-final.pdf)r

## Surveillance Trust – Surveillance Controller Registry

The WG Co-Chair Salvatore D’Agostino, also Founder of Surveillance Trust B-Corp, applies the TPS to make records of processing to enable notice and consent for utilizing AI in video surveillance. The controller Record is registered to become a Surveillance Controller Operator credential for the operators of video surveillance systems. Applied in functions that use machine learning for scene characterization, personal identification, and individual characterization.

We would like to continue to work through the liaison between Kantara and ISO to contribute to our work and look forward and engage further the security, privacy and identity industries in this new trust framework that enables real human consent. Thank you for the opportunity to participate.