**Transparency Trust Metrics**

Editors: Mark Lizar

Contributors:

**IPR Option:**

This ANCR Record Specification is required to be open is specified under a Reasonable and Non‑Discriminatory (RAND) agreement at the Kantara Initiative for submission to ISO/IEC SC 27 WG 5

Presented for assessing conformance of the Transparency Code of Conduct(ref), for implementing the Council of Europe 108+ Chapter III, Rights of the Data Subject, Section 1 Transparency and modalities Article 14, 1 – 8. Internationally representative of notice and consent legal and social requirements, represented today with the privacy policy link, CCTV Sign, mandatory security or privacy notices, found when accessing public and, digital service spaces, in all domains and jurisdictions, referenced as practices, which implement, or support the implementation of this code of conduct.

As a result, a special consideration, that this TPI specification MUST not have any dependency, that is not open, accessible, and available for public interest, digital transparency and consent technologies.

.

This specification relies on (open access to) ISO/IEC 29100 Security and privacy techniques, to generate a notice receipt, which is stored in a consent record, ANCR record format for conformity assessment. Utilizing the Kantara Initiative Consent Receipt v1.1

Patent & Copyright: Reciprocal Royalty Free with Opt-out to Reasonable and Non-discriminatory (RAND)

**Suggested Citation: (upon WG approval)**

ANCR Specification v0.9

NOTICE

This document has been prepared by participants of Kantara Initiative Inc. Permission is hereby granted to use the document solely for the purpose of implementing the Specification, for public benefit. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce this document, in whole or in part, for other uses must contact the Kantara Initiative to determine whether an appropriate license for such use is available.

Implementation or use of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third-party intellectual property rights. This Specification is provided "AS IS," and no Participant in Kantara Initiative makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third-party intellectual property rights, or fitness for a particular purpose. Implementers of this Specification are advised to review Kantara Initiative’s website ([A picture containing graphics

Description automatically generatedKantara Initiative: Trust through ID Assurance](http://www.kantarainitiative.org/) ) for information concerning any Necessary Claims Disclosure Notices that have been received by the Kantara Initiative Board of Directors.

Dear reader,

Thank you for downloading this publication prepared by the international community of experts that comprise the Kantara Initiative. Kantara is a global non-profit ‘commons’ dedicated to improving trustworthy use of digital identity and personal data through innovation, standardization and good practice.

Kantara is known around the world for incubating innovative concepts, operating Trust Frameworks to assure digital identity and privacy service providers, and developing community-led best practices and specifications. Its efforts are acknowledged by OECD ITAC, UNCITRAL, ISO SC27, other consortia and governments around the world. 'Nurture, Develop, Operate' captures the rhythm of Kantara in consolidating an inclusive, equitable digital economy offering value and benefit to all.

Every publication, in every domain, is capable of improvement. Kantara welcomes and values your contribution through [membership, sponsorship](https://kantarainitiative.org/membership/) and active participation in the [working group](https://kantarainitiative.org/groups/isi-work-group/) that produced this and participation in all our endeavors so that Kantara can reflect its value back to you and your organization.

Copyright: The content of this document is copyright of Kantara Initiative, Inc.  
© 2023 Kantara Initiative, Inc.

Introduction

Transparency Performance Indicator’s (TPI’s) are introduced here as the object of conformity, captured to capture the presentation of PII Controller credential information, to determine the operational capacity of the information in conformance Conv 108+ and personal expectations.

The TPI are used to create and ANCR (Anchored Notice and Consent Receipt) which is a record that is presentable as a ‘proof of notice’ claim, the object for both conformity, and compliance assessments, which are presented in this scheme.

TPI scheme, to test the performance of digital transparency with a privacy request, tests how dynamic the performance of transparency and consent is for data subject rights, independently of the service provider, relative to context.

The 4 TPI’s presented here pinpoint 4 metrics that can be used to measure the conformance of transparency and the integrity of consent in a data capture context.

Assessing the operational capacity of required PII Controller Identity and Contact presentation. Measuring the performance of the publicly required digital service information. Checking digital components of authority and security to assure and assess the validity of privacy.

The ANCR record, is a capture of digital governance and surveillance context, and it is anchored with proof of knowledge. Capturing the point of presentation of PII Controller ID, and privacy rights access point, and the digital governance framework to which personal data processing is being governed.

The ANCR record, in which the PII Principle is the holder and controller of this record, can be presented as a micro-notice claim and credential to engage PII Controller privacy services to capture the PII Controller performance.

Most assessment for conformance of privacy information or services are mapped to analogue legal requirements which measure response times in days, out of technical context.  TPI’s all measure how dynamic privacy service information is in context, and provides a rating, from -3 to +1, in which +1 is for a Dynamic, in context transparency performance indicator, introducing an active state transparency measure for capturing dynamic digital transparency and consent performance, for the first time.

cyber physical security and digital privacy through the decentralized authority inherent in the Notice Record.

Why was this specification written?

* Give up privacy to access privacy service
* No record of digital relationship
* No receipt for consent

At the time of writing this specification, transparency and consent is governed predominately by commercial governance frameworks that utilize digital identity management technologies to identify people, without identifying themselves in a standard way online, which compliant and conformant, presenting critical cybersecurity risks.

These risks are exacerbated when PII Principals use privacy services online, as PII identifiers are captured and collected at an attribute level (known also as meta-data), which means individuals must relinquish their digital privacy, to access online privacy services. As these technologies themselves are used to profile and track data subjects presenting systemic obstacle to accessing privacy services in a meaningful way for the PII Principal.

The second systemic obstacle being that individuals do not have their own records for digital identity relationships, which prevent people from data controls that are autonomous, subjecting them to terms and condition for privacy access. The ANCR record is used to address this systemic challenge, with a proof of knowledge, legal claim for data subject access rights.

What’s more, an ANCR Record, can be used to generate consent notice receipts, to enable the individual to direct a primary and secondary consent in any given context. Which is the focus of the ANCR Record Framework (ref)

Why Transparency Performance Indicator’s?

Currently, there is no way for people to see who is tracking them and to understand how digitally exposed one is, in any given physical/digital surveillance context. Data control, access to digital privacy information for consent, to test to see what consent ( privacy rights) requests response times are.

TPI’s indicate if the digital information provided upon contact with a digital service is capable of meeting this basic requirement and capable of dynamic data access and controls.

Digital transparency around purpose of use, who benefits, how and where data is processed, is extremely important security and privacy session attributes information, used in the TPI scheme assessments. Without standardized approach to the presentation of digital transparency it is difficult if not impossible to make decisions about the creation and subsequent necessary, tracking and monitoring of personal data and digital identifiers.

TPI’s conformity and compliance assessment for digital transparency can then be useful to dramatically improve the safety, security, privacy usability and awareness for people in context measuring the operational performance of digital privacy at the moment.

What should you expect to find in this document?

The presentation of 4 Transparency Performance Indicators, which capture transparency and data capture practices in context, to test the self asserted information for its operational usability.

TPI’s specified focus on the initial point of contact. The publicly required information that MUST be provided, referring to the PII Controller Identity and Contact information which is required in all privacy legal instruments. Transparency in this regard is a universal requirement, and required for free, prior and informed consent to scale online.

The TPI’s here are used to assess session based data capture and self asserted information by organizations, referred to as Level of Trust Assurance 0, in the ANCR record framework. Which means the TPI report, provides the same level of assurance as a privacy policy link or page does on website, or a sign. In which there is no additional assurance of the validity of the PII Controller information provided.

Note to reader: The ANCR Record Framework presents 4 levels of transparency assurance for PII Controller Notice Credentials, which can be use in 3 vectors if digital governance, 1. Personal data control 2. Data Protection 3. Co-regulation, which is what is assessed in this document at the public assurance level 0.

TPI 1 - Measuring the Timing of PII Controller Identity Notification:

This TPI captures when the Controller's legal entity and accountable Privacy Officer (digital identifiers) provide notice of their identity; measuring if it is

1. Before,
2. At the time of,
3. During
4. or After personal data is captured.

Assessing how dynamic and operational transparency to provide a way for an individual to assess if they can trust a service or not. Assessing compliance with Article 14.1, specifically defined in Article, 15 1, a) and b)

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a)  the identity and the contact details of the controller;

(b)  the contact details of the data protection officer;

Note: This is the most common legislated privacy element in the world, required and mappable to all privacy legislation and instruments. [(ISTPA 2007)](https://kantara.atlassian.net/wiki/spaces/WA/pages/2916489/Auxiliary+Reference+Documents?search_id=d979240f-f5c8-42e3-8c8c-5dbd2dd748d0)p.64

TPI 2 - Measures Required Data Elements

This TPI captures the data elements required for all data processing (except when legally regulated otherwise [3] derogation). In “all” cases a Notice of who is processing your data, who is a accountable and the privacy contact information for access to personal information is required to be *provided*. [Art 14.1]

Specifically, a first time notice must include 2 factors, 1) is notice credential 2) is the practices relating to permissions

Digital Privacy transparency elements:

1. Legal Entity Identity Name,
2. Address, Contact information
3. Name or role of Data Privacy Officer (or the authoritative owner and Accountable Person (AP) in charge of that legal entity
4. Privacy services access and contact point information
5. Privacy or other Governance Policy Governing the processing of personal information
6. Transparency before use
   1. Legal Basis and Purpose for Processing
   2. Recipients or categories of recipients if Any
   3. Transfer of data on networks out of Country, to a 3rd Country, and the existence of adequacy, existence of safeguards, where to get a copy of them, or where they have been made available.(note)
7. Transparency required to be available in context, during the time when PII is obtained (found in Transparency Statement or Privacy Policy [note]
   1. Period of time data stored
   2. Existence of rights/controls to access and rectify
   3. Existence of right to manage consent
   4. Existence of right to lodge a complaint with a DPA
   5. Whether processing is based under a statutory, or contractual context or whether necessary for entering a contract, if the PII is obliged and the consequences of failure to provide this data,
      1. Note: (Added by Editor) and who controls access to the authoritative version of the data processed.
   6. Existence of
      1. AI, or any Automated decision making technology,
      2. digital identity management surveillance technologies
      3. any profiles generated
      4. Meaningful information about the logic involved, [Note]
         1. its significance
         2. Expected consequences for and to Data subject

\*\*\* edited to here \*\*

TPI 3 - Measure of Transparency Accessibility

This TPI measures the performance of transparency accessibility by capturing how the availability of the required information in TPI 2. For example, is the information presented in a pop-up notice, or is it required to click a link, e.g. to a standard transparency/privacy policy, is it the first screen or is it at a the bottom of a multi-screen display (with links not highlighted).

TPI 4 - Measures security information integrity

This TPI captures the (Secure Socket Layer/Transport Layer Security) SSL/TLS ([e.g. 1.3](https://datatracker.ietf.org/doc/rfc8446/)) certificate or security keys ([e.g. JOSE](https://datatracker.ietf.org/group/jose/about/)) to compare its meta-data against the required information in TPI 2. This is very much along the lines of [Certificate Transparency](https://certificate.transparency.dev/) but looking specifically at whether the policies cover the Notice, e.g. does the SSL certificate Organization Unit field and Jurisdiction fields match the captured legal entity information, how does the policy and jurisdiction here related to other beneficial entities. Importantly does this align with the policy expectations of the person.

TPI Metrics

move for intro text

TPI’s are captured in sequence;

1. TPI measuring the point when the individual is notified versus when personal information/digital identifiers are collected and processed. Capturing the timing of notice presentation in relation to first data capture

2. TPI measuring the contents of the notification for required PII Controller digital attributes that correspond to the physical brick and mortar attributes specified in privacy, security, safety and surveillance legislation. This is the Controller identity and entity information and access point

3.TPI for how accessible the transparency is (transparency of digital transparency)and the accessibility of the notice access for use

4.TPI validating the cybersecurity information versus the digital transparency information capturing the SSL certificate or keys and its associated meta-data.

Combined, these TPI’s provide an overall Indication of the operational state of digital privacy.

TPI Methodologies

Timing of Notice vs Data Collection Transparency

TP1 requires monitoring the technical end point to see if PII is captured in relation to when a notice is provided. This measures the notice regulatory performance against legal and human usability requirements.

PII Controller Digital Attribute Transparency

Assess if the required information for transparency over who is in control of notice is ‘provided’

The MUST fields identify elements that are required in legislation that MUST be present.

Transparency Accessibility

How accessible is the PII Controller and Privacy Contact information?

For example, in the context of a website or a mobile device, how difficult was it to access the ‘provided’ information. How many clicks, or screens, away is the required information?

**Example — Accessibility Measurement Rating**

This transparency accessibility rating score of [1,0, -1 or –3] reflects the number of steps, screens, or clicks required to find the ‘provided’ information within a mobile application or webpage providing the client user interface.

Security Validation Certificate (and/or Key) Security Transparency

This security performance indicator requires that the session security layer certificate or key information to be collected and then compared against the information in the Notice Record to validate the integrity of the security necessary for digital privacy.

This checks if the PII Controller identity information is the same or linked to the controlling entity in the associated security certificate. For example, does the SSL certificate identify the Controller, and is it secured for the DNS and localization expectation and corresponding jurisdictional information. This provides required digital security for privacy, measured for governance accountability and interoperability with legal adequacy with for eConsent (electronic or digital consent).

Certificate status, and transparency performance, are used to establish session security prior to the collection, use and processing of PII. The security TPI also measures the certificate and or cryptographic keys for a specified organizational unit to corroborate and validate the PII Controller’s digital integrity.

Table 1: Transparency Performance Rating

The TPI Rating system is designed to measure the operational performance of the information. This rating is unique as it allows for an assurance levels that account for pre-assured, dynamically assured metric.

+1 refers to a technical framework and PII Controller transparency prior to the initiation of a session providing security based trust assurances.

0 refers to dynamic a measure of providing dynamic transparency in the context of once a technical session starts (which is at the time of collection), in context transparency over purpose and disclosures,

-1 provides for analogue legal expectations, represented by legal requirements not specific to a digital context.

-2 provides for low quality provision

-3 provides a metric for non-operable transparency and digital privacy.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rating** | **TPI 1 - Timing (wrt to processing)** | **TP2** | **TPI3 Accessibility (trans performance)** | **TPI4 - digital security** |
| +1 (assured) | Before [Transparency of control/governance - Before, during or after processing ] | +1 - credential is registered and present | Controller identity is presented prior to data collection - e | Security is required prior to collection (digital wallet based) |
| 0(dynamic assurance) | Just In time | 0 credential is presented just in time (automated check and first time notice) | Embedded as a credential linked to authoritative registries. | is assured -e.g. certificate is specific to and matches controller and context |
| -1 (analogue assurance - online) | During | controller information is accessible during collection | PII Controller Identity prominently displayed on first view – prior to processing first page of viewing, the assessment question would be | not-specific to controller - does not match jurisdiction |
| -2 - (not mandatory in flow) | Available | Controller information is linked | is linked not presented | does not match ou |
| - 3 ( non operative) | After | Controller information not present | Identity or credential is not accessible in context - e.g. two or more screens of view away, or privacy contact is mailing g address and non operative in context of data collection. | is not valid or secure provider |

TPI Instruction and Guidance

The TPI Rating system is designed to measure the operational performance of the information, for example if only a mailing address is provided for a privacy contact, on a website, this is considered non-operable according to the context. This means that privacy access and specific information is not retrievable in the context of data collection. Demonstrating a non-performant form of data governance.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rating - Instruction** | **TPI 1 - Timing (wrt to processing)** | **TP2 - Required Info Presentation** | **TPI3 Accessibility (trans performance)** | **TPI4 - Digital Security** |
| +1 (assured) | PII Controller credential is displayed, using a standard format with machine readable language and linked, for example, in an http header in a browser | Controller is discoverable automatically prior to session (out of band) in a machine readable format. Number of ways  1. is a Controller Identity Trust registry  2. is client side record of processing (via a wallet or browser) | Controller identity is presented prior to data collection | Security is required prior to collection (digital wallet based) |
| 0(dynamic assurance) | PII Controller Identity or credential is provided in first notice | 0 credential is presented just in time (automated check and first time notice) | Embedded as a credential and dynamically available upon access (almost just in time) | is assured -e.g. certificate is specific to and matches controller and context |
| -1 (analogue assurance - online) | The Controller Identity, or screen with the Controller Identity is one screen and click away. For example, the privacy policy link in the footer of a webpage | controller information is accessible (not presented) during collection | PII Controller Identity prominently displayed on first view – prior to processing first page of viewing, the assessment question would be | not-specific to controller - does not match jurisdiction |
| -2 - (not mandatory in flow) |  | Controller Credential information is linked during collection | is linked not presented | does not match ou |
| -3 ( non operative) | PII Controller Identity is not accessible enough to be considered ‘provided’ | Controller information not present | Identity or credential is not accessible in context - e.g. two or more screens of view away, or privacy contact is mailing g address and non operative in context of data collection. | is not valid, secure, or recognized provider.  Not security operational (proving non reciprocal security assurance) |

Table 2: TPI Schema

|  |  |  |
| --- | --- | --- |
| TPI 1 |  |  |
| Notification Timing |  |  |
| Timing of Data Collection |  |  |

Table 3 : Transparency Performance Indicator Record Rating Example

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Field Name** | **Field Description** | **Requirement: Must** **Shall** **May** | **TPI 1**  before (out of band), just in time (before), at the start - or time of collection, during collection and after collection | **TPI 2**  **Available**  **Not Available** | **TPI 3**  **Rate: +1, 0, -1, -3,** | **TPI 4** **Certificate or Key**  **CN-Matches** **OU – Match** **Jurisdiction – Match (optional)** |
| Notice Location | Location the notice was read/observed | MUST | before, during, after | Present | +1 | found |
| PII Controller Name | Name of presented organization | MUST |  | Present | 0 | Match |
| PII Controller Address | Physical organization Address | MUST |  | Present | 0 | Not match |
| Privacy Contact Point | Location/address of Contact Point | MUST |  | Present | 1 | Not match |
| Privacy Contact Method | Contact method for correspondence with PII Controller | MUST |  | Present | -1 | No Match |
| Session key or Certificate | A certificate for monitored practice | MUST |  | Present (or Not-found) | 1 (or –3 ) | Present (or No Security Detected) |

Summary

In summary, Transparency Performance Indicators, TPI’s are specified here for people to use depending on context, location, security, and other out of session elements. TPI’s are used to determine with one's own soverign reasoning whether to trust a service, not an external framing, opinion or forced default.

These TPI’s use open standards, with an open license specified for people to be able to use and create records they can own and keep across and independently of service providers.

TPI 1 is a measure of trust, so that when asked, “Do you trust (accept) a service”, you necessarily know who is processing your data before, during or after.” Overwhelimingly people indicate trust would be higher. if notified prior to data capture, which only makes sense.

TPI 2 is the legally required information, is it present, and then used as a, generally available, standardized, and open metric for compliance.

TPI 3 is an indicator for how accessible and inclusive is digital transparency.

TPI 4 validates for the individual if security “adds up” for the them and in doing so addresses a critical security gap widely overlooked today.

Roadmap

References

Appendix A: Notice Record Schema

In this appendix, here is a notice record template to fill out when recording a rating, along with a rating template, and analysis results format.

Notice Record Schema & , Notice Record and Report - Template and Example

1.2.    TABLE1: NOTICE RECORD SCHEMA

|  |  |  |  |
| --- | --- | --- | --- |
| FIELD NAME | FIELD DESCRIPTION | REQUIREMENT: MUST, SHALL, MAY | FIELD DATA EXAMPLE |
| Notice Location | Location the notice was read/observed | MUST | [Walmart.com | Save Money. Live Better](http://www.walmart.com/) |
| PII Controller Name | Name of presented business | MUST | Walmart |
| Controller Address | The physical address of controller and/or accountable person | MUST | 1940 Argentina Road Mississauga, Ontario L5N 1P9 |
| PII Controller Contact Type | Contact method for correspondence with PII Controller | MUST | Email, phone |
| PII Controller-Correspondence Contact | General contact point | SHALL | [Privacy@org.com](mailto:Privacy@org.com) |
| Privacy Contact Type | The Contact method provided for access to privacy contact | MUST | email |
| Privacy Contact Point | Location/address of Contact Point | MUST | [Org.com/privacy.html](http://org.com/privacy.html) |
| Session Certificate | A certificate for monitored practice | Optional | SSL Certificate Security (TLS) and Transparency |

Endnotes

1 Lizar, M, Pandit, H, Jesus, V, “Privacy as expected Consent Gateway”, Next Generation Internet (NGI) Grant [Access July 4] privacy-as-expected.org/