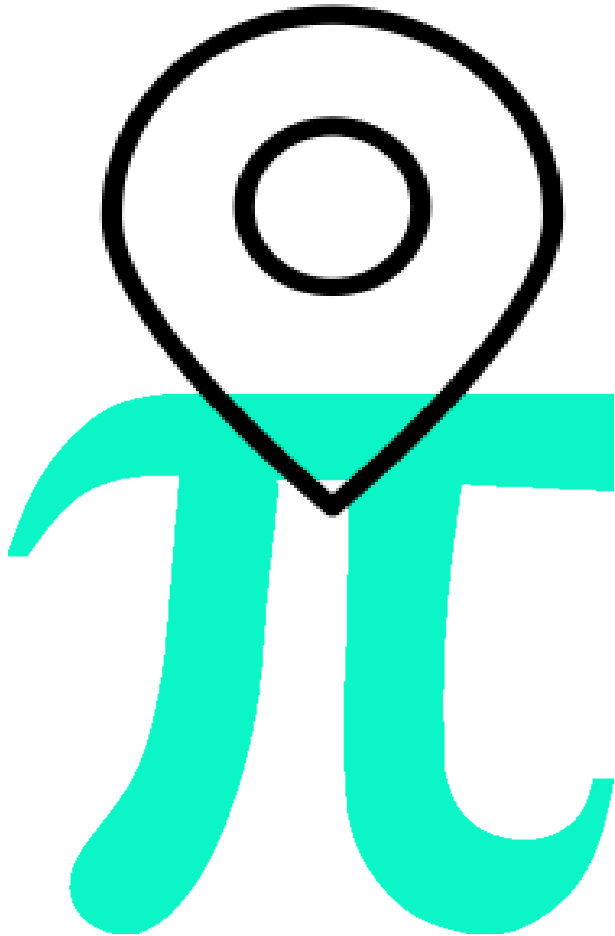


PII Governance





Starts Here

The Premise

Protection of Personal Identifiable Information (PII)

- **A Data Subject is defined as an identifiable natural Person** – Data Subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person’s physical, physiological, genetic, mental, economic, cultural or social identity. In other words, a data subject is an end user whose personal data can be collected.
- **Personal Identifiable Information (PII)** - PII is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
- **Entitlement to PII (ENT)** – A Data Subject (individual) owns the rights to their PII, which includes the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to a decision based solely on automated processing. These “Rights” are an asset of value and may be likened to the rights to access a “Property” (or “Product”) owned by the Data Subject. Accordingly, a Data Subject may grant access, via an entitlement to an entity (either Business or Private), to one or more rights to access their PII under the terms of a predefined agreement.
- **Protection of PII** – The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. Government or Commercial Entities that may have access to personal identifiable information concerning individuals and other sensitive data have a specific responsibility to protect that information from loss and misuse.
- **As a result, to protect against the misuse of PII by any Government or Commercial Entity** a mechanism can be implemented whereby a Data Subject may *“Grant to the Entity an Entitlement for Specific and Measurable Rights to use the Data Subject’s PII”* whereby such access and usage against entitlement may be measured and made available to both parties with systematic trust, via an Entitlement Management Capability using a Permissioned Blockchain Ledger (EMS-BC).

The Pitch

Personalization & Privacy Concerns 2026

- **The Elephant in the Room: AI** – Digital experiences are becoming AI-driven and hyper-personalized.
- **Personalization requires increasing amounts of user data:** The potential to infer sensitive information, such as a person's location, preferences, and habits, poses risks of unauthorized data dissemination.
- **Regulation and consumer distrust are rising:** Coupled with the potential for identity theft and unwarranted surveillance, AI presents a unique set of challenges that demand immediate proactive solutions
- **Current experience platforms (AEP, Salesforce Data Cloud, HubSpot, etc.):** All optimize experiences for companies. The next generation will optimize experiences with the consent and governance of the user.”

Digital Experience Platforms Need a Trust Layer

Governed PII Management

Anatomy of the Governed PII Life Cycle

- **Information Life Cycle** - The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion. *(DHS.gov Handbook for Safeguarding PII)* The Controller is responsible for
- **PII Controller** – The PII controller is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of PII. The Controller has primary responsibility for compliance with PII regulation and demonstrate that the process is performed in compliance with that regulation. These measures should be considered as follows:
 - The nature, scope, context, and purposes of the processing
 - The risks of varying likelihood and severity for the rights and freedoms of natural persons because of any processing
- **PII Processor** - Processors must meet certain PII management requirements even if not defining why and how that PII is processed. Data processors act in the interest of the data controller, meaning that the processor is serving the controller’s interest by carrying out their PII tasks under the governance of the controller. Processors are responsible for:
 - Processing PII in accordance with the instructions provided by the Data Controller;
 - Receiving the consent of the Data Controller prior to using any subcontractors;
 - Have a contract with the Data Controller;
 - Demonstrate compliance with the requirements of GDPR and all other governing rules for PII
 - Implement appropriate security measures.

A Simple Example Scenario

Willow Has Some fun

Personalization & Privacy Concerns 2026

- **The Elephant in the Room: AI** – Digital experiences are becoming AI-driven and hyper-personalized.
- **Personalization requires increasing amounts of user data:** The potential to infer sensitive information, such as a person's location, preferences, and habits, poses risks of unauthorized data dissemination.
- **Regulation and consumer distrust are rising:** Coupled with the potential for identity theft and unwarranted surveillance, AI presents a unique set of challenges that demand immediate proactive solutions
- **Current experience platforms (AEP, Salesforce Data Cloud, HubSpot, etc.):** All optimize experiences for companies. The next generation will optimize experiences with the consent and governance of the user.”

Digital Experience Platforms Need a Trust Layer

An Example Scenario

Willow Has Some Fun

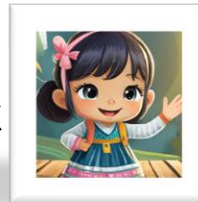
Data Subject “Willow” visits the Fun Park

“Curiosity Driven”

- **Willow** sees a sign at the entrance saying... “*For a fun time download our FunApp*” which she found quite funny... so she did (*with Daddy’s help!*)
- **FunApp** spoke to **Daddy**, “*Tell me something about Willow, Daddy*”,  to which Daddy responded:
 - “*Willow is five, loves trains, hates loud noises.*”
 - “*Keep her on gentle rides only.*”
 - “*No scary content.*”
 - “*No location sharing beyond the park.*”
 - “*Today is her birthday, so prioritize special kid-friendly experiences.*”
 - “*Delete everything when we leave.*”
- Then **FunApp** spoke to **Willow** and said, “*Follow me to the train Willow!*” and **Willow** followed the directions,  then rode the train
- When **FunApp** saw **Willow** had completed the ride it asked **Willow** if that was fun and would she maybe like to ride on a very gentle live pony? 
- To which **Willow** proclaimed with an excited squeal... *oooh YES!* 
- And **FunApp** guided **Willow** to a quiet ride on a pony picked out especially for her age group
- ..and this went on all day 



Until **Willow** came to the end of her day & exited the Fun Park



Bye Bye !!

Possible Outcomes

This is broader than FunApp

- The same pattern works for:
 - children’s online games
 - educational apps
 - AI companions
 - social platforms
 - healthcare portals
 - travel experiences.
- Anywhere a person says:
 - “Here is what this user is allowed to experience.”
- The PII-Track AI agent can help translate that into policy.
- PII-Track also provides Systematic Trust with Secure PII Access Auditability for both the Enterprise Service Provider AND the Consumer.

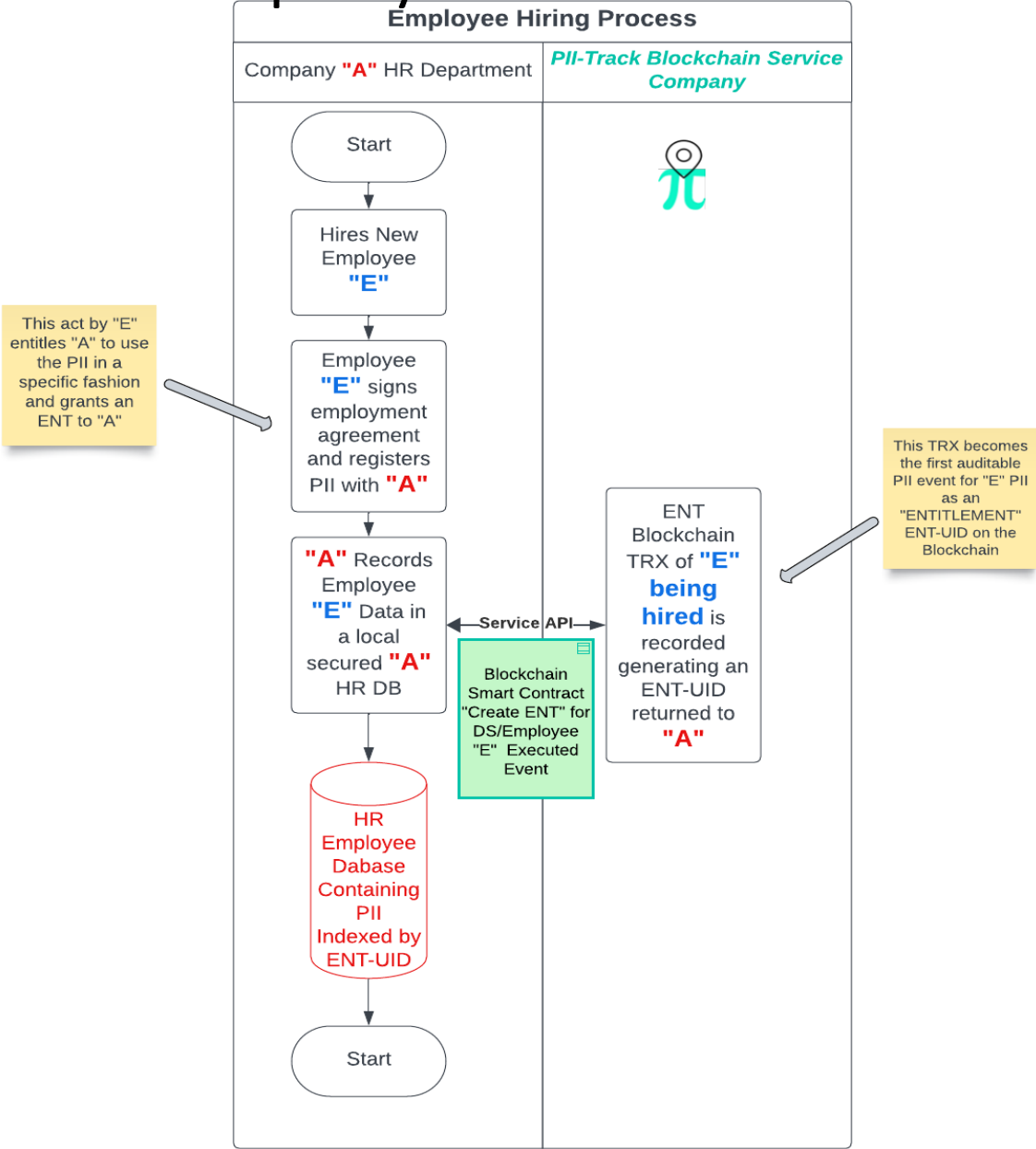
A customizable digital experience with a transparent contract between the user and the platform, governing how the experience works

A Business Example Scenario

Employee HR Services

Company "A" Hires Employee "E"

"Curiosity Driven"

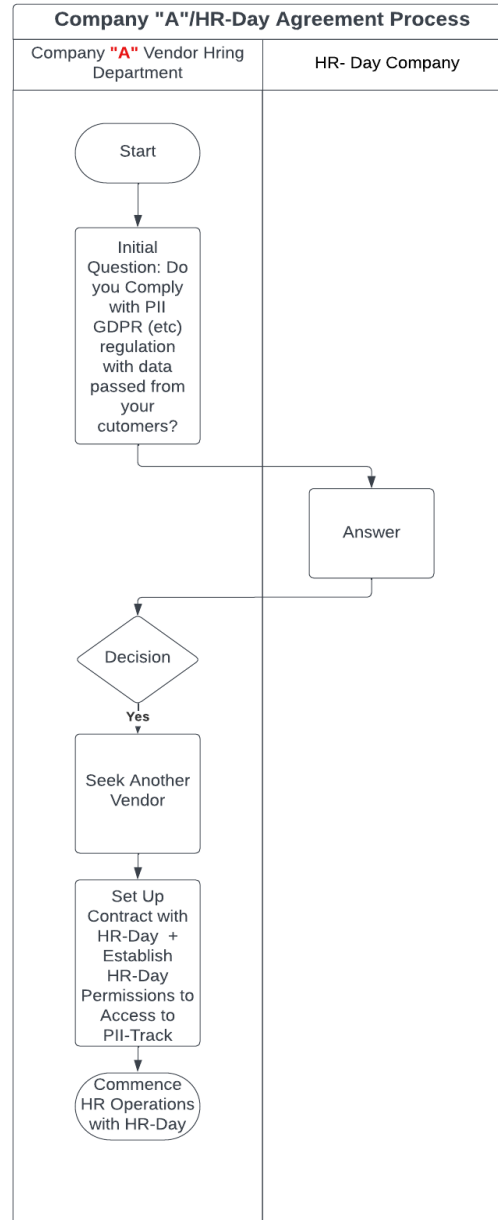


Company "A" Works with "HR-Day"

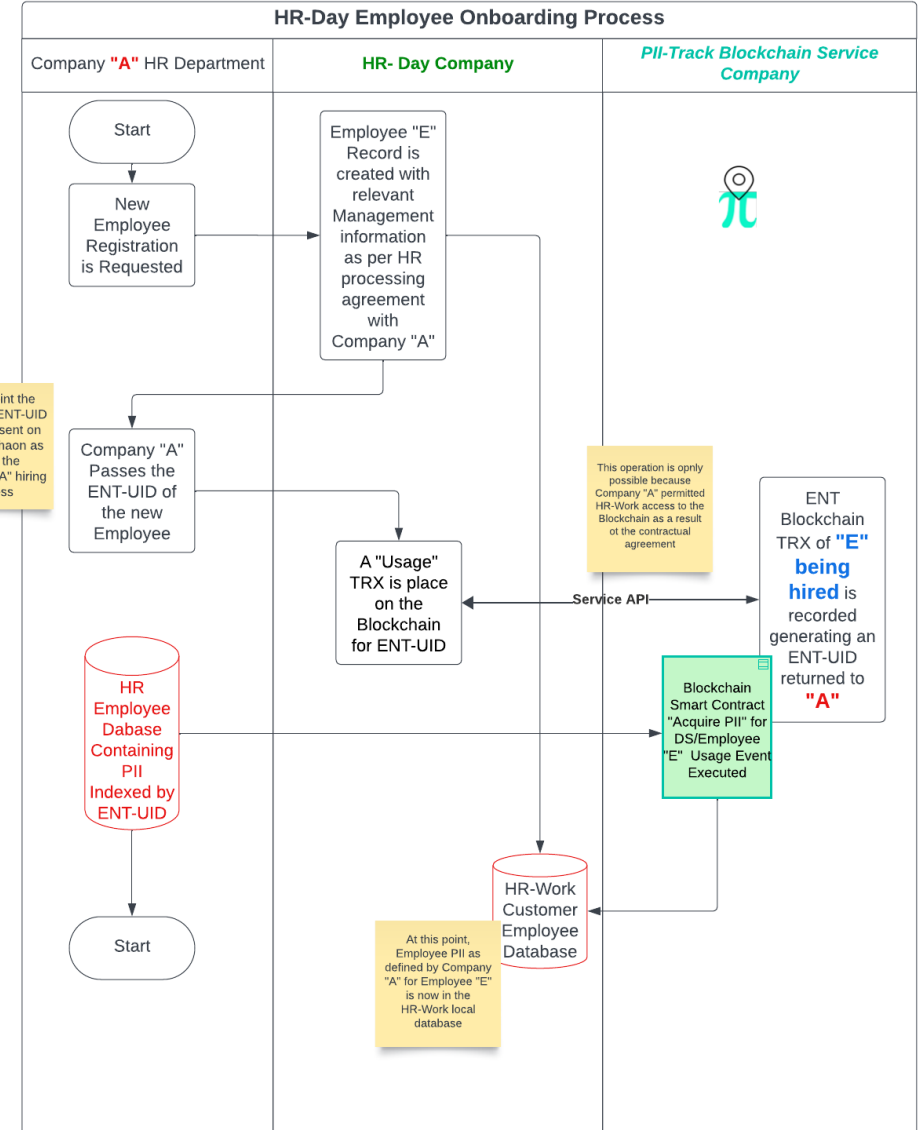
(an HR Service Organization)

"Curiosity Driven"

- Company "A" must set up a working relationship with "HR-Day" before processing may begin.
- Part of that relationship must be a commitment to comply with any PII "Controlling Requests / Orders" that are made to to HR-Day will result in the outcomes as defined by "Company A"'s PII processing policies.



- This is an example of Company "A" requesting an action to be executed by HR-Day via an API call. This is the initial call, but all HR functional calls such as "Terminate Employee", "Promote Employee", "Change employee Role", etc., requiring local PII changes follow the same pattern.
- The assumption is that HR-Day must have received the appropriate PII compliance commitments from its operating partners with respect to managing PII. Thus HR-Day can pass on any appropriate Company "A" commands on DS PII management, such as "Change Attribute" or "Delete" as per PII legallyrequired compliance.



Use Cases

The PII-Track PII Life Cycle Use Cases

Use Case 4: PII Archival Stage

Upon cessation of the **Controller** or **Processor's** use of a Data Subject's PII, as defined by the entitlement:

- The PII is transformed for archiving such it may still be managed according to the associated entitlement yet also be used for statistical purposes
- The transformed PII may not reveal the identity of the Data Subject without the assistance of the Data Subject e.g., in the case of a Data Subject's DSAR request

"Curiosity Driven"

Use Case 5: PII Destruction

- PII Inventory and Mapping allows destruction to be precise and auditable
- Destruction can be driven via multiple policies, e.g., via blanket policies and/or PII entitlement policies, optimizing for maximum protection of the **Controller**, all **Processors** and the Data Subject

Use Case 3: PII Transfer

- A transaction is created recording the event of a request to transfer **Controller** managed PII for use either to a **Processor** within the **Controller** infrastructure internally, or to a **Processor** external to the **Controller** which MAY be allowed if:
 - The request for use is within the terms of the "Data Subject's Grant of Entitlement"
 - Any jurisdictional differences in requirements between source and destination are met

Use Case 2: PII Usage

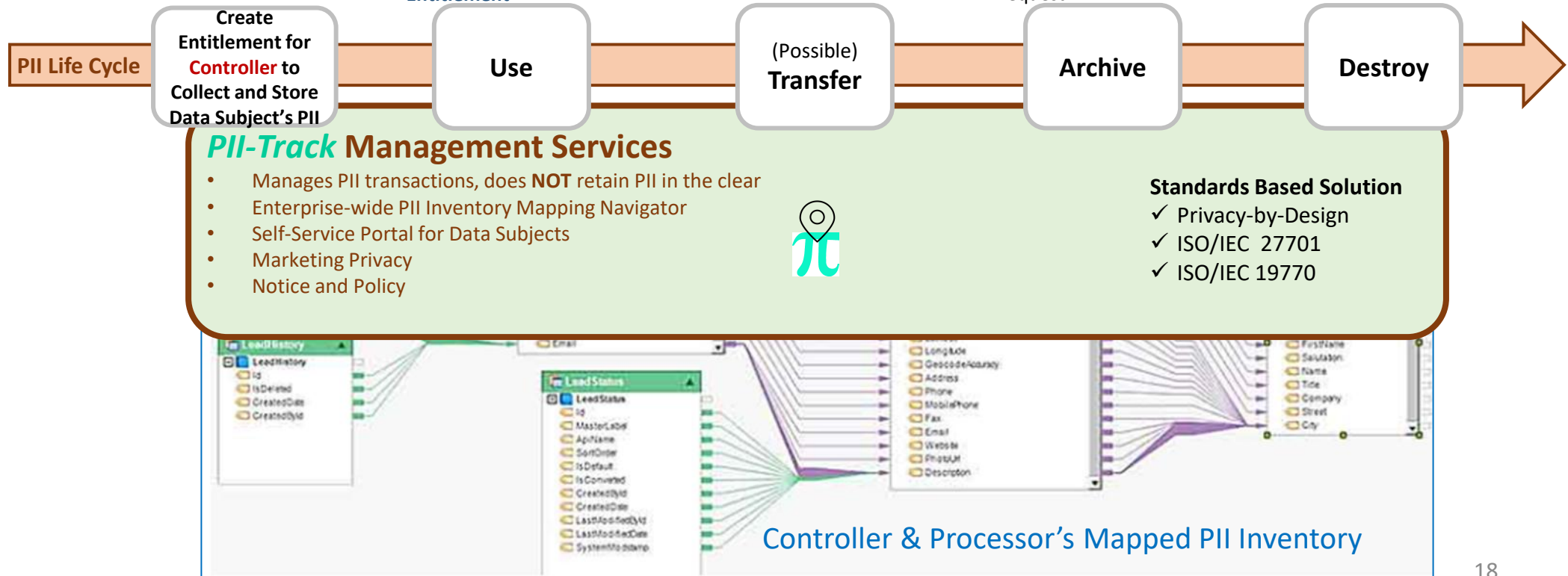
- A transaction is recorded of the **Controller's** PII access requested and the action allowed if usage/access of the Data Subject's PII falls within the "Data Subject's Grant of Entitlement"

Use Case 1: Consent Management

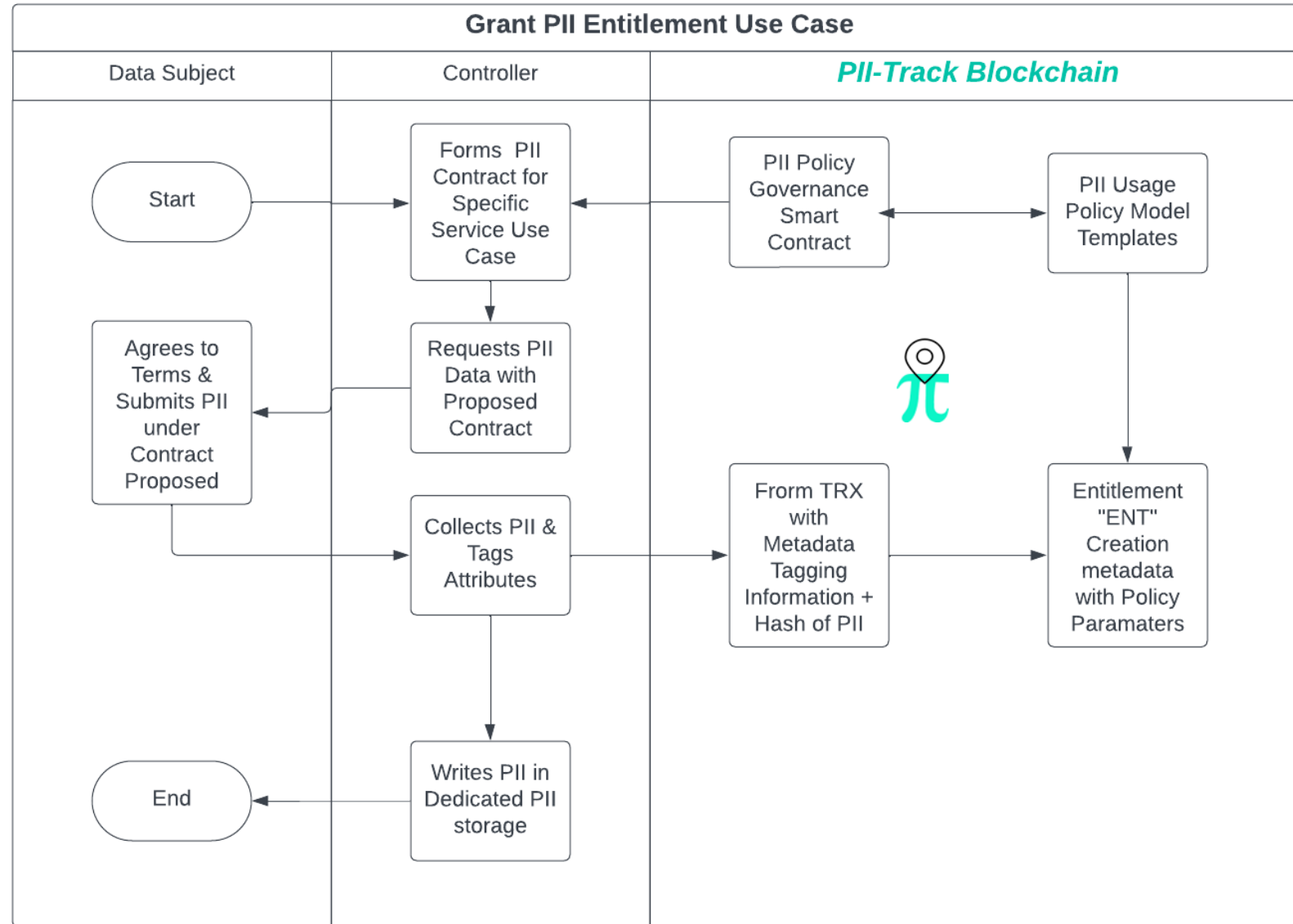
- A transaction is recorded of "Data Subject's Grant of Entitlement" for the **Controller** to Collect, Store and Use their PII, as per terms proposed by the **Controller**

Data Subject Use Case

- Authorized entities (i.e., the Data Subject, their proxy or agent) may inquire on a specific Data Subject's PII entitled usage, actual usage, status or deletion / destruction at any time during the life cycle, including post destruction verification

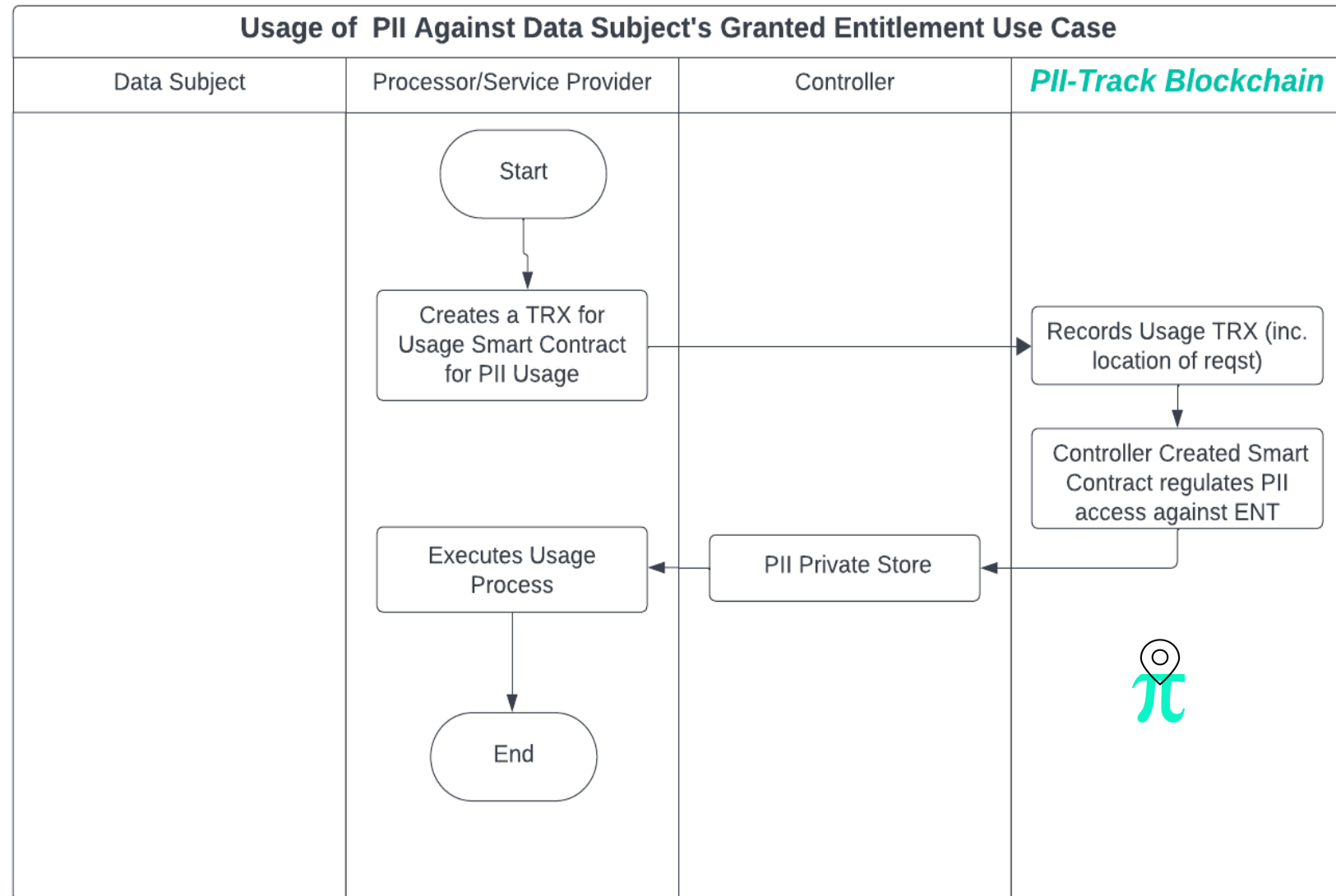


Data Subject Consents to Grant Entitlement for PII Use

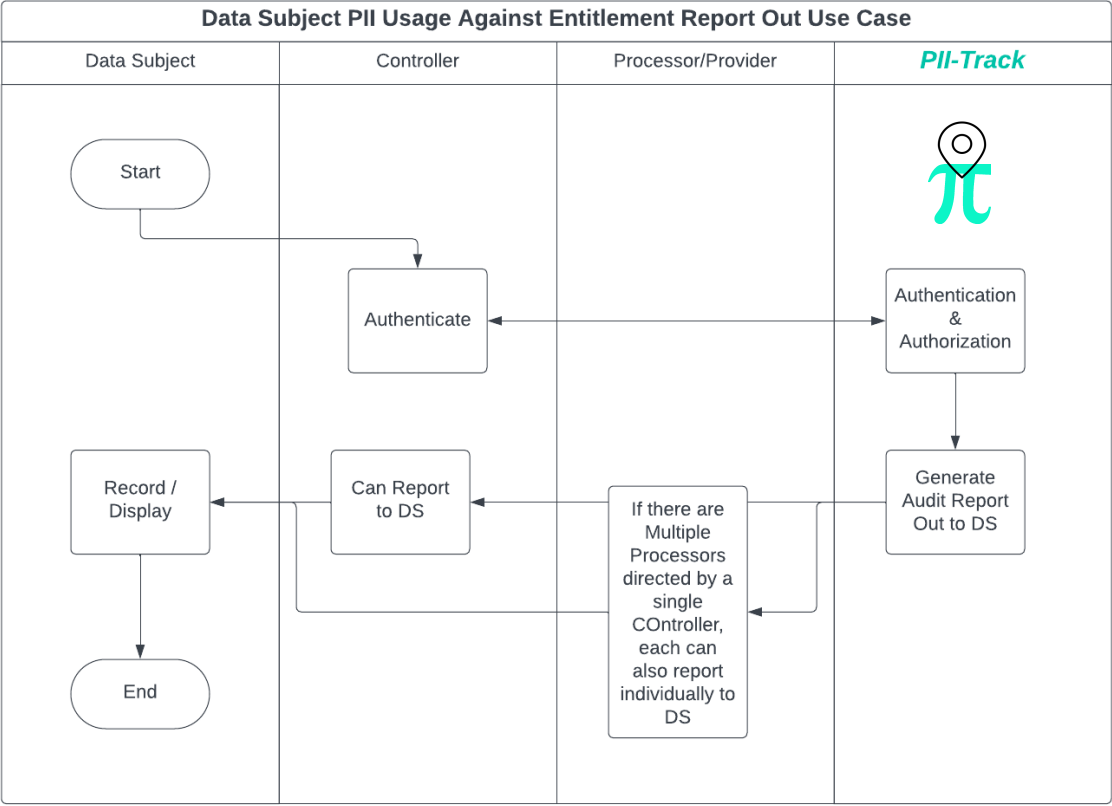


Processor's Usage of PII against Data Subject's Grant of Entitlement

"Curiosity Driven"



Data Subject’s Report on Any/All Service Processor’s Usage Against Grant of Entitlement



PII Life Cycle Report					
Service	Collect	Use	Archive / Copy	Destroy	Possible Violation
Service Name	Attribute(s) + Policy + Date/Time	Attribute(s) + Action + Date/Time	Attribute(s) + From + To + Date/Time	Attribute(s) + Action + Date/Time	"
"	"	"	"	"	"
"	"	"	"	"	"
"	"	"	"	"	"
"	"	"	"	"	"

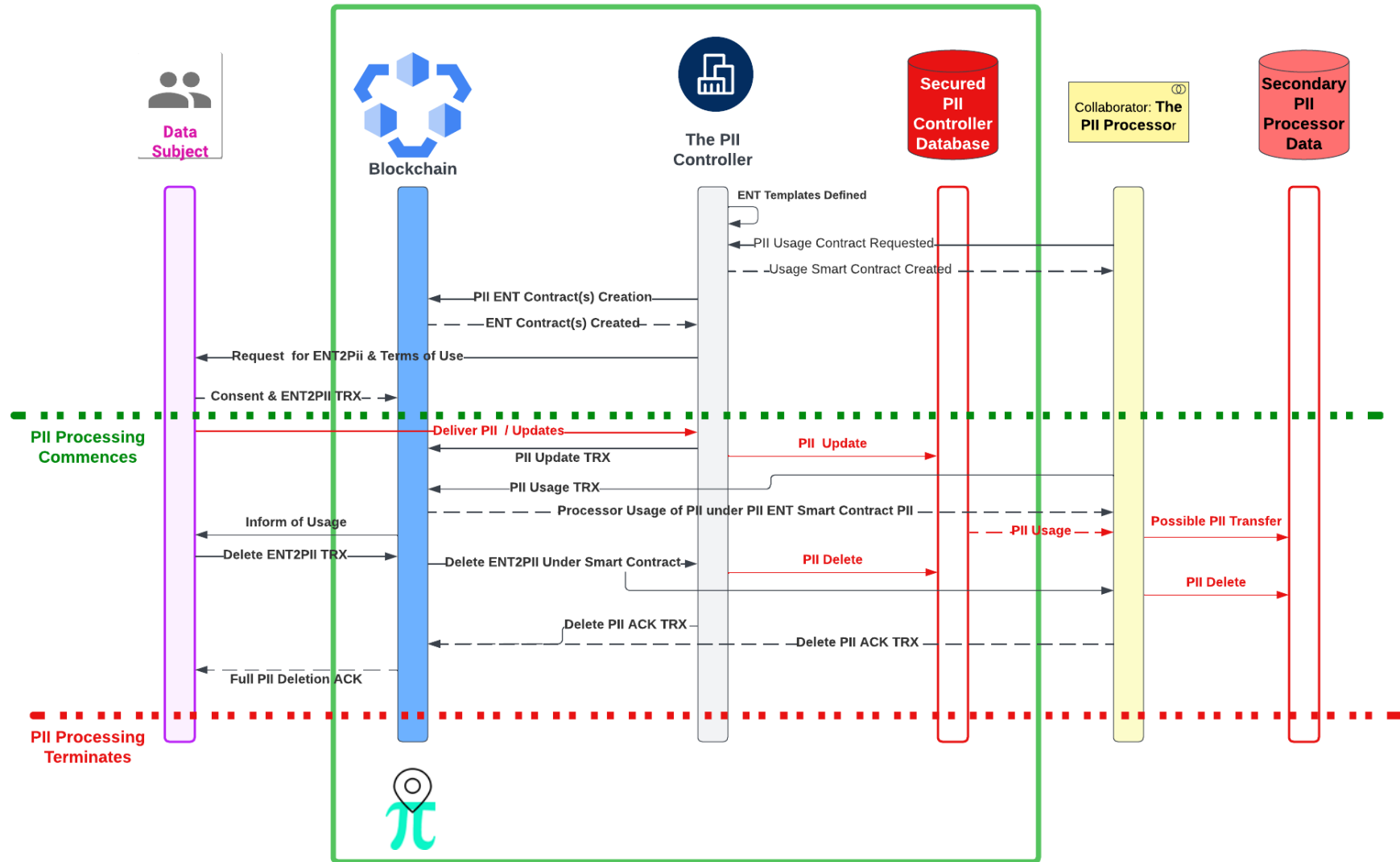
Identity monitoring agency feed

Architectural Concepts

The PII-Track General Sequence Model

"Curiosity Driven"

- **The Controller** manages all processing via the use of Blockchain smart contracts which it alone may manage in the permissioned Blockchain
- **The Processor** manages all processing via smart contracts which are managed only by the Controller and thus the outcomes are governed by the Controller.
- All processing by the **Controller** and/or the **Processor** is tracked immutably and auditable on the Blockchain



Functional Concepts of an EMS-BC

Critical Permissioned Blockchain Capabilities

- **Permissioned blockchains:** Allow for selective data visibility, ensuring that the information is only accessible to only authorized participants.
- **Controlled Participation:** The level of participation (such as the ability to read, write, or audit the blockchain) is also controlled, and different permissions can be assigned to different users
- **Identity Management:** Participants in a permissioned blockchain have known identities, and their roles and access levels within the network are well-defined.
- **Smart Contracts:** Are programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met. Within a smart contract, there can be as many stipulations as needed to satisfy the participants that the task will be completed satisfactorily. To establish the terms, participants must determine how transactions and their data are represented on the blockchain, agree on the “if/when...then...” rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes.

The Entitlement Management Model

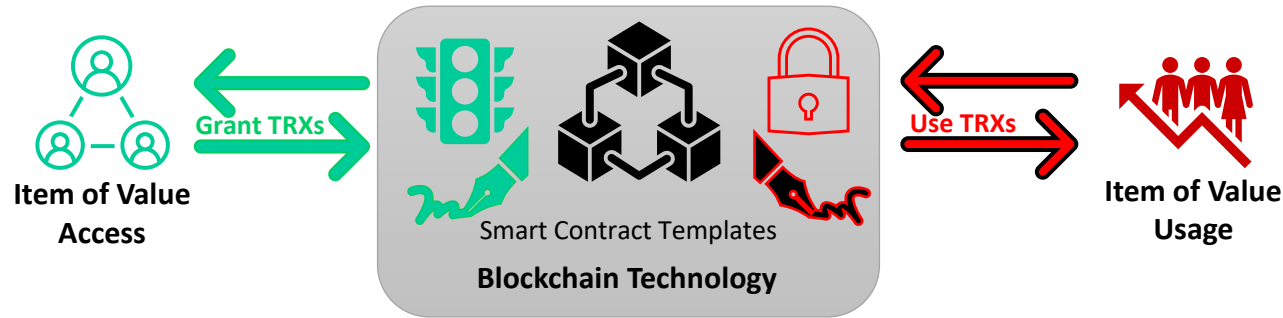
- **Consider the Concept of an “Item of Value”** that is possessed / owned by an entity or individual by virtue of being the item’s creator or being legally acquired from another entity or individual.
- **The Item of Value** may be tangible or intangible. For instance, the tangible Item might be a physical object or goods such as an automobile or building. An intangible Item might be some form of intellectual property (IP) such as the master copy of a digital photograph, the master copy (digital or physical or otherwise) of a story or novel, or indeed the original design for an intangible or tangible item.
- **The Item of Value** may also have value to some other entity(ies) or individual(s) by virtue of its potential use or application in their own context.
- **The Owner of an Item of Value**, may grant rights to use their Item in some very specific and well-defined manner without the need to relinquish ownership of the Item. For instance, the automobile as a tangible Item may be rented to a 3rd party for specific uses as governed by the Rights, the building may also be rented or leased to a 3rd party in the same way. A 3rd party may also be granted specific rights to use an intangible Item, by being given access to the Item such as digital read access for use to the digital photograph, or the story or novel, or the design mentioned above.
- **The Rights Granted** to the 3rd parties then each become an Intangible Asset with an associated value for each Right(s) which the owner may have granted, usually in exchange for some asset of an equal value.

Thus, when a 3rd party is granted Rights to use an Item of Value, the 3rd party owns an “Entitlement to Use” the Item of Value, albeit ONLY under the terms of the Rights granted

The Blockchain Entitlement Patent

The Blockchain Applied to Entitlement Management

“Curiosity Driven”

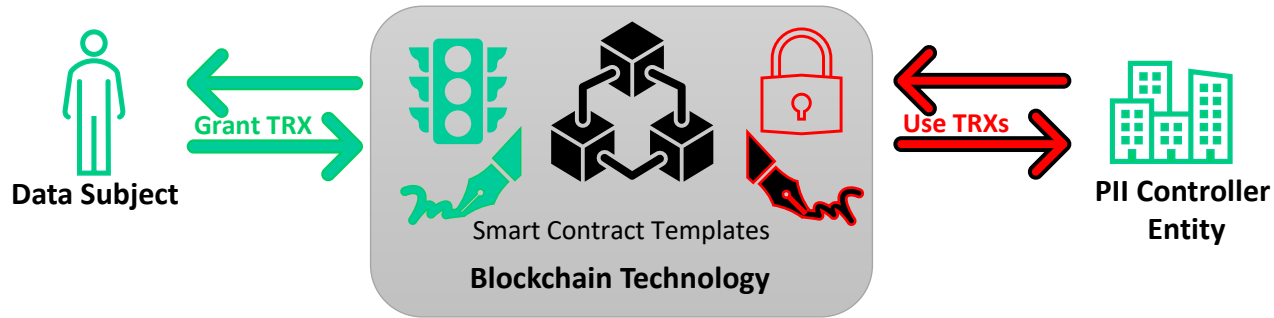


- **The Grantor / Grantee of Entitlement Relationship of Trust** – The opposing goals between the grantee(s) and grantor of entitlement for maximizing value from the acquisition and associated sale of rights to use an Item of Value can discourage trust between the parties.
- **Trust** – A Permissioned Blockchain provides three systematic capabilities that will help guarantee trust:
 - Secured shared access to the Entitlement and Usage information distributed between parties that wish to establish a relationship of trust.
 - With the use of cryptography, that shared data is immutable, i.e., cannot be deleted or altered other than by incrementally adding to the information.
 - Smart Contracts, also contained on the Blockchain, can be created by the Grantor of the Entitlement(s) that systematically manage Grantee execution of Blockchain Usage transactions that are created because of systematic integration with Usage of the Item of Value entitled. The Smart Contracts can be configured to match any legal agreement between Grantee and Grantor.
- **The Systematic Application of Blockchain Trust & Functionality to Entitlement Management**
 - Grantees and the Grantor can understand the 1:1 relationship between the transaction driven systematic execution of smart contracts and any commercial contract formed between the parties.
 - Grantees & Grantor can have real-time visibility into both Entitlement and Usage information, ensuring an open understanding and expectation of value to both.
 - The immutable transaction information of entitlement and usage data across time enables provision of secure audit information to the grantor and grantee(s) across time, even when entitlements or Items of Value are changed, exchanged or renewed, by virtue of the patented transaction “Container” capability built upon the Blockchain.
 - The patented data “Template” model that has been developed allows any form of Entitlement, containing any number or configurations of Rights to define Blockchain Smart Contracts suitable for Rights management of any Item of Value, both tangible and intangible.
 - The patented “Template” capability allows both the Grantor & Grantee(s) to add a new, renew or change the individual Rights contained within any Entitlement, at any time and subsequently, the feature Use available, at any time merely by updating the “template” that drives smart contract policies without requiring any material changes to the Blockchain based solution.



Providing Systematic Trust with Secure Entitlement & Usage Auditability for both the Grantor AND the Grantee of Entitlement of Rights Use an Item of Value

The Blockchain Entitlement Management Applied to Privacy ^{“Curiosity Driven”}



- **A Data Subject is defined as an identifiable natural Person** – Data Subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person’s physical, physiological, genetic, mental, economic, cultural or social identity. In other words, a data subject is an end user whose personal data can be collected.
- **The Item of Value** in this Use Case is **Personal Identifiable Information (PII)** - PII is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
- **The Grantor** in this Use Case - A **Data Subject** (individual) owns the rights to their PII, which includes the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to a decision based solely on automated processing. These “Rights” are an **Item of Value** and may be likened to the rights to access a “Property” (or “Product”) owned by the Data Subject. Accordingly, a Data Subject may grant access, via an entitlement to an Entity (either Business or Private), to one or more rights to access their PII under the terms of a predefined agreement.
- **The Grantee** in this Use Case – Is the PII Controlling Entity that is requesting access to the PII for whatever reason.
- **The Predefined Agreement** – In this use case will be defined by the Entity and must be clearly defined to the Data Subject and formally accepted prior to Granting Entitlement to Use of the PII to the Entity. This could include Rights including time-period of Entitlement, attributes granted access, any changes to PII as requested by the **Data Subject**, all metrics associated with Usage, etc.. The Predefined Agreement must be implemented as a Smart Contract which systematically governs the management of the Entity’s Usage of PII, including the method of Use and defined location of storage.
- **Associated Local and Global Regulation of PII** will be included as a component of the predefined agreement (subsequently implemented in the appropriate Smart Contracts) including agreement on changes to the agreement because of changes in regulation at any time.

Providing Systematic Trust with Secure Entitlement & Usage Auditability for both the Grantor AND the Grantee of Entitlement of Rights to Use a Data Subject’s PII

Conceptual Business Approaches

Current Solutions

Data Governance Processors (DGPs)

- [Collibra](#), [Atlan](#), [osano](#) & [Alation](#) (there are others) currently provide functionality that allows their enterprise users to tag and govern data (including PII) across their end user’s infrastructure
- These companies have already, to some extent, sold the concept of providing PII management assurance to their customers, i.e., enterprise end users, as they provide PII “metadata tagging” and data lineage tracking
- They have **NOT** provided any capabilities to their enterprise end user’s customers, i.e., the data subjects (DSs) themselves, to manage, monitor & regulate how their PII is used during its life cycle by the enterprise end user.
- Nor have the current data governance tools provided an audit trail of how the PII is used / consumed within the enterprise end user’s infrastructure.

Is there is then a value proposition for DGPs to partner with openthinka (OT) as that audit partner to offer value to both DGP’s enterprise end user corporations as well as their customers, i.e., the Data Subjects ?

If so, there is NO Current Solution available other than the [patented](#) solution we propose

Possibly Partnerships with DGPs to Enterprise Customers

If we (OT) believe that the DGPs have already cracked the enterprise end user’s desire for PII governance nut, then [Collibra](#), [Atlan](#) & [Alation](#) (and others) currently provide would be our entry point, as partners, with any enterprise that might benefit from the added value OT provides:

- DGP’s Enterprise end user / customer’s self auditing of PII management, access and usage, by PII element, by known Data Subject
- Increased satisfaction for the Enterprise’s own customers either by
 - Allowing direct access to data subject access requests (DSRs) via the OT portal
 - Or proving automated & audited reporting and management of the DS’s PII on request

dwright@openthinka.com