ARTICLE TITLE - OWNERSHIP AND FLOW PRIMITIVES FOR SCALABLE CONSENT MANAGEMENT IN DIGITAL PUBLIC INFRASTRUCTURES

ARTICLE AUTHORS – ROHITH VAIDYANATHAN, DEV SHINDE, PRASEEDA, SRINATH SRINIVASA

PRESENTER'S NAME AND AFFILIATION – DEV SHINDE (RESEARCH SCHOLAR @ INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY BANGALORE)

PRESENTER'S EMAIL ADDRESS – SHINDEDEV.HEMRAVI@IIITB.AC.IN

Myself Dev Shinde

Topics of Interest – Digital Public Infrastructure, Cross Border Data Exchanges, Intelligent System Designs

Current Working on Building framework for Internationalization of DPIs and building automated compliance framework for Cross Border Data Exchanges

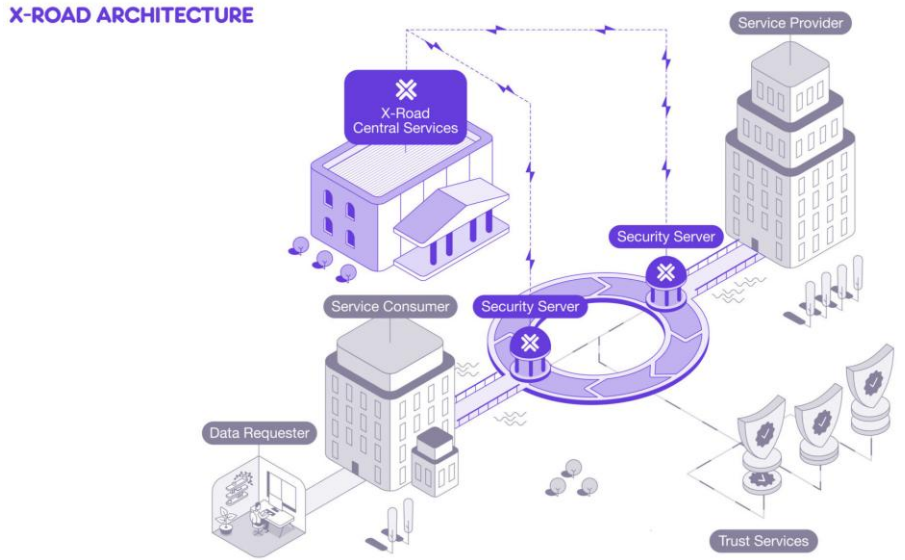
DIGITAL PUBLIC INFRASTRUCTURES

1) DPI represent open ecosystems of digital services, applications and assets made available for public good

2) DPI services like digital identity, lockers, catalogs, wallets and payment infrastructures have not only empowered e-governance– connecting governments to the public, but also a variety of economic, legal and social transactions among ordinary citizens

DigiLocker
Your documents anytime, anywhere

3) DPIs are digital infrastructures that handle ***private data*** and they use this private data to provide services for public benefit



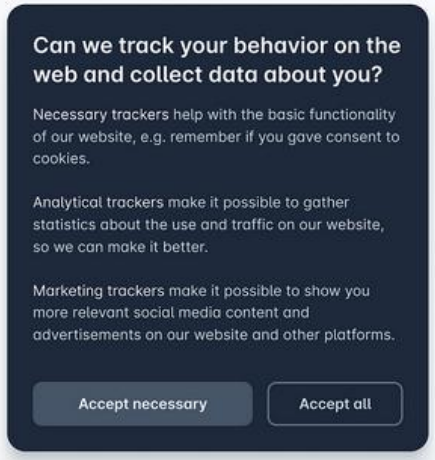
4) Increased interoperability of public data between public and private entities

“PUBLIC” INFRASTRUCTURE HANDLING “PRIVATE” DATA

1) Soliciting sensitive data is often legitimate and necessary for providing services to citizens.

2) Here, Data Owners (DO) often lose track the downstream custody of their data and how their data is used.

3) Thus, a key principle is user consent - data should be accessed or shared **only with explicit/ implicit, informed/ implied and revocable consent** from individuals.

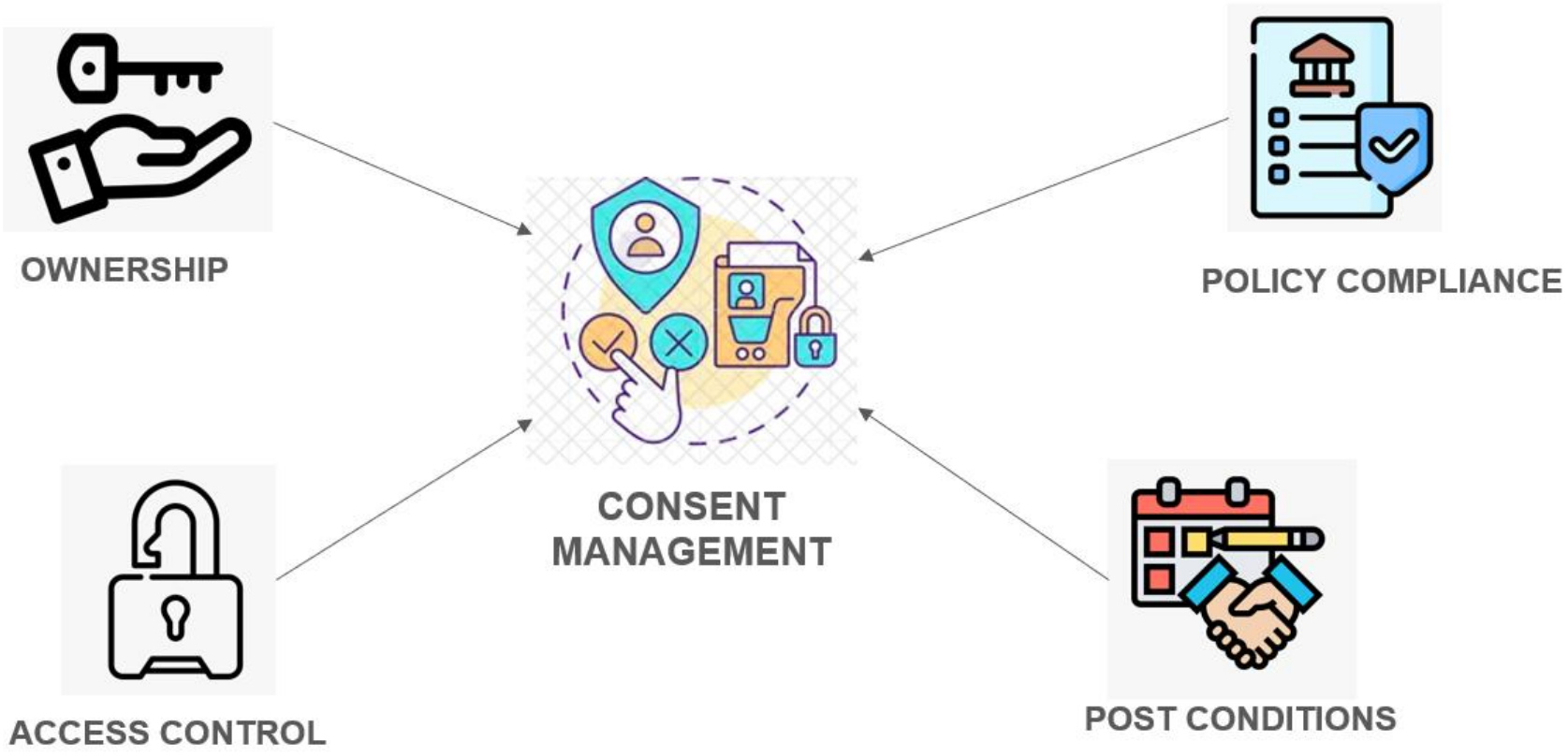


WHY CONSENT AND OWNERSHIP IS INTERTWINED DEALING WITH PRIVATE DATA

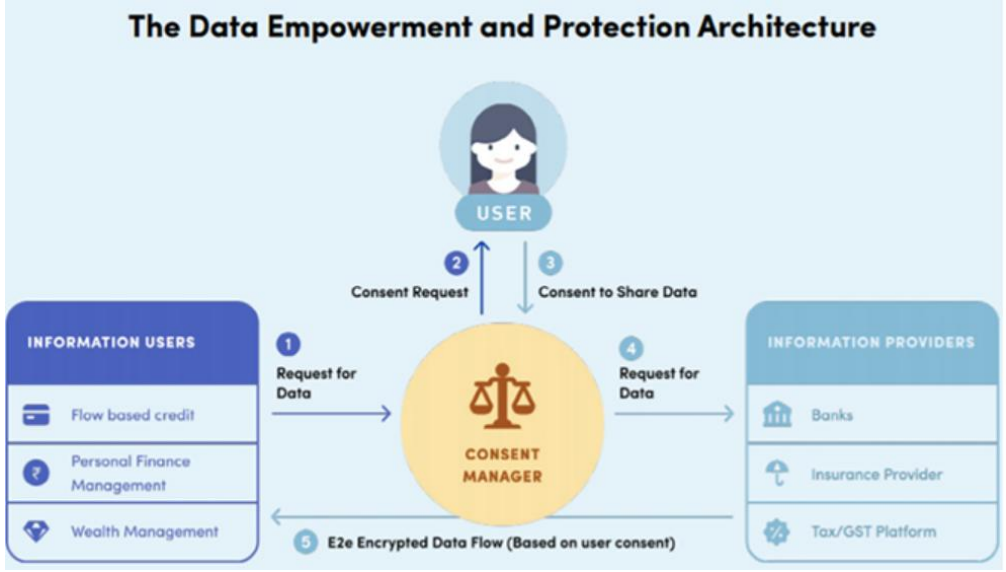
1) One can give consent, for only what one “owns”. Here, consent for data sharing is closely tied to data ownership.

2) One example, imagine your degree certificate issued by your college. You own that degree as it is yours, but you can’t change anything on it. And college can also revoke it (So, this is an instance of where ownership is shared, *conferred ownership*)

DIMENSIONS OF CONSENT MANAGEMENT



DATA EMPOWERMENT PROTECTION ARCHITECTURE (DEPA)



1) Consent management is modelled as an interception of a data flow, to ensure that the flow is consistent with the consent of the data owner.

2) Employs Autonomous Authorisation (AA) model, involves an explicit consent signal to be sent by the Data Principal (consent giver) in response to an access request. The DO is clearly asked, and they clearly respond (e.g., by ticking a box, signing digitally, or approving via an app).

3) As DPIs scale, frequent Requests would lead to consent fatigue or consent desensitisation - where the data owner may not adequately understand the implications of her choices (As we saw in our previous example, we are also victims to this).

4) If there is a Data Custodian – He/ she cannot autonomously approve, he will need to adhere to some data sharing policy set by the DO.

SOME EXISTING INITIATIVES

1) Traditional Access Control Models – RBAC [1-3], ABAC [4, 5] and hybrid RBAC/ ABAC models [6, 7] – These models often model with attribute relationships between the Subject and an Object and have a consistent system of logic to resolve access requests.

2) An alternative model called the Fair Transaction Model [8], proposes legitimately implied consent, which overcomes the issue of consent transaction overload in the AA model. Policy Based Consent Management [13] is an implementation of the Fair Transaction Model, evaluates and enforces regulations and data sharing policies.

3) The question of consent is closely related to issues of ownership, and the consideration of individual or collective autonomy. On these lines, there have been studies on what makes consent meaningful and other philosophical works [9, 10].

4) Regulatory developments around consent management – Indian DPDP, GDPR, European Data Governance Act [11, 12].

Clearly Issues of consent goes beyond access control

SOME EXISTING INITIATIVES

1) Several Data Exchanges have come up recently, to handle open ended public data (personal and non-personal) lawfully.

2) Some of them use ownership registration systems – assumes complete authority of data asset to the DO [14].

3) In Web3, ownership of digital assets is managed using Non-Fungible Tokens (NFTs) that are stored on an immutable ledger like blockchain.

4) Storing an NFT on a permissioned blockchain can be an enabling mechanism for asserting ownership, but there is still a need for representing and enforcing the semantics and legal implications of ownership and its morphological forms (like delegated ownership, leased ownership etc) [15]

Does sharing of data constitute sharing or transferring of ownership to the recipient, and what data flows can one legitimately control by virtue of ownership ??

IUDX

TERMINOLOGIES

Agent: Agents or Stakeholders assert ownership on the data and play different roles like Data Owner (DO), Data Requester (DR) or Data Subject (DS)

Lockers/ Access Policy Domain: They represent semantic boundaries like containers where data ownership is enforced. An agent can own one or more lockers.

Connection: A data flow interface between a pair of lockers that represent legitimate pathways by which, data can be exchanged between different stakeholders. Connections are made legitimate by an underlying contract encapsulating the data sharing policies of the respective stakeholders, as well as applicable regulations.

Connection Type/ Connection Endpoint: A connection type is a schema that specifies terms and conditions, under which a connection can be established between the lockers of two agents. It can be imported from a template or can be built from Data Owner data sharing policies

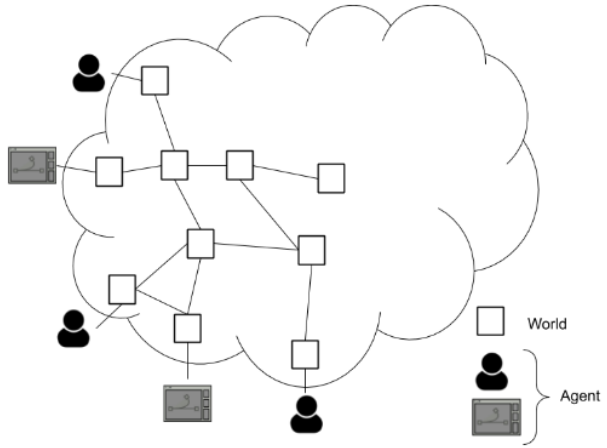
MODELLING AN ARCHITECTURE FOR DPI

A -> A is a set of agents or stakeholders who assert ownership

W is a set of containers representing semantic boundaries– called as Access Policy Domain (APD)

$$DPI = (A, W, F)$$

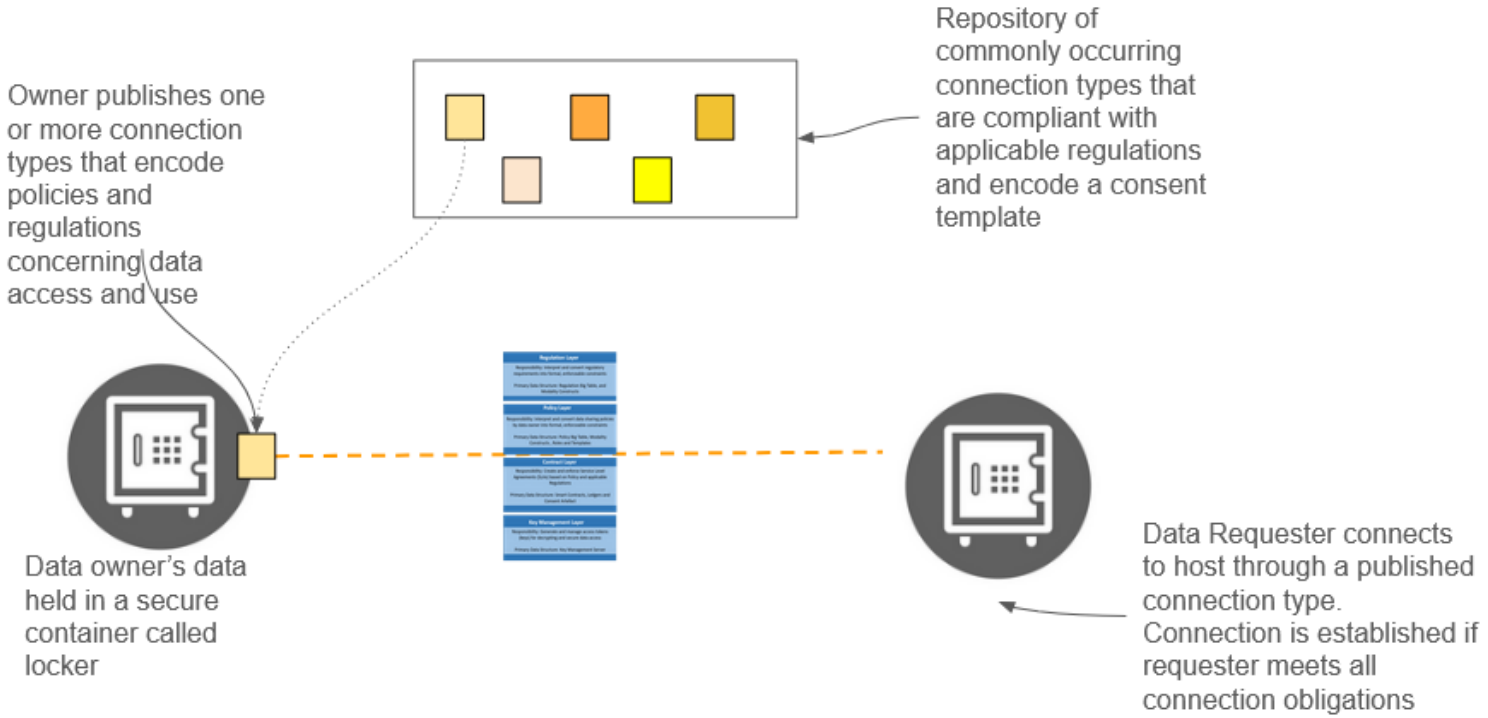
$F \subseteq W \times W$ - represents data flow pipelines– also called Connections– established between lockers that represent legitimate pathways by which, data can be exchanged between different stakeholders and are based on a contractual template.



For any given locker $w \in W$ and agent $a \in A$, if agent a wishes to access some artifacts that are available in locker w' belonging to agent a', then a first connects to a suitable endpoint published by w' presenting w as the participating locker from its side. Once the agreement is established, this leads to the formation of links $(w, w'), (w', w) \in F$

In a broad sense, data in a DPI may be thought to be in one of three fundamental states: data in rest, data in use, and data in transit. Consent management primary applies to data in transit. Data in transit refers to connections between any two data storage locations, or connection between a data storage and an application that processes the data

DEPICTION OF A CONNECTION



Regulation Layer

Responsibility: Interpret and convert regulatory requirements into formal, enforceable constraints

Primary Data Structure: Regulation Big Table, and Modality Constructs

Policy Layer

Responsibility: Interpret and convert data sharing policies by data owner into formal, enforceable constraints

Primary Data Structure: Policy Big Table, Modality Constructs , Roles and Templates

Contract Layer

Responsibility: Create and enforce Service Level Agreements (SLAs) based on Policy and applicable Regulations

Primary Data Structure: Smart Contracts, Ledgers and Consent Artefact

Key Management Layer

Responsibility: Generate and manage access tokens (keys) for decrypting and secure data access

Primary Data Structure: Key Management Server

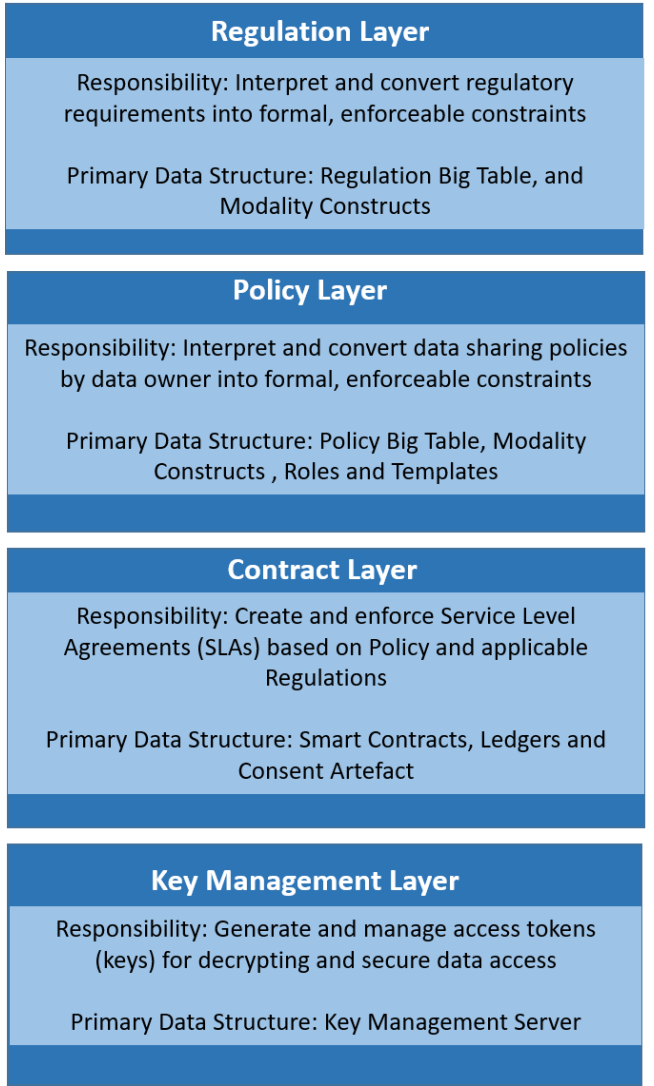
4 LAYER CONSENT SERVICE ARCHITECTURE

Regulation Layer - Regulatory provisions are obtained from applicable legal documentation. Data access policies may be bound by such regulations specified in one or more applicable regulatory sources. They are stored as **ECMA** (Event-Condition-Modality-Action) rules.

Policy Layer - Analogous to regulations, data sharing policies have an applicable extent that defines the boundary of the organization or community called **Lockers.** Locker rules are augmented with rules inherited from all the applicable regulatory sources with regulations receiving higher priority.

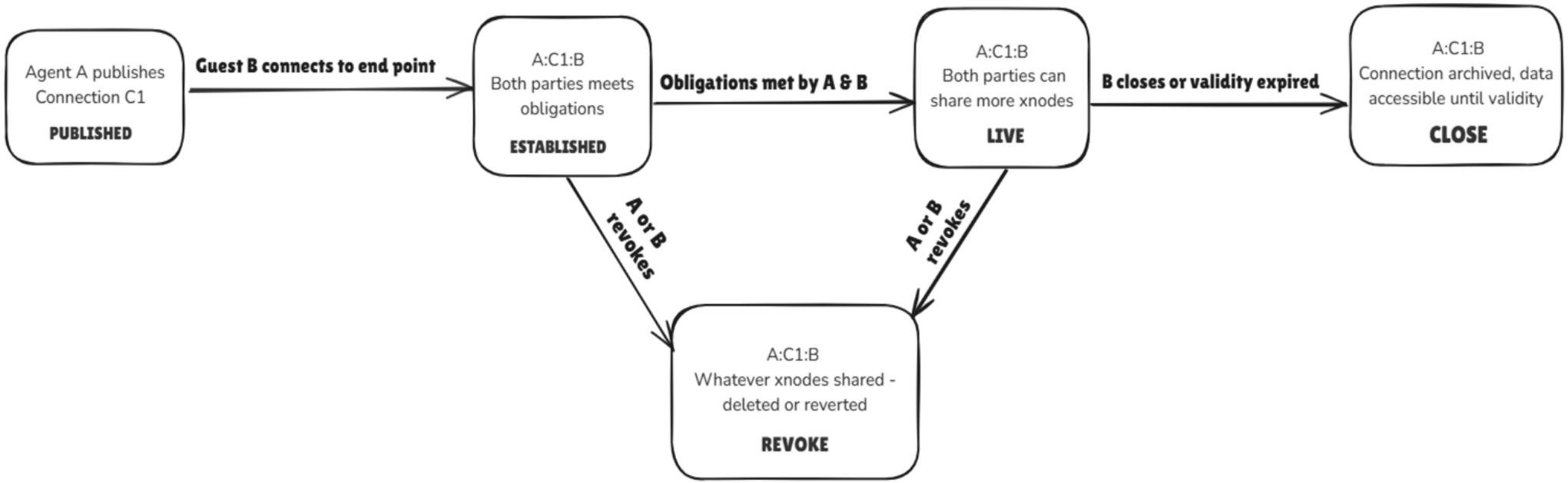
Contract Layer **-** The contracts layer helps in enforcing the rules present in the **consent artefact** after data access has been granted to the data requester.

Key Management Layer **-** Consent Managers are required to be **data-blind** and are not allowed to themselves read the data being shared.



Balambiga Ayappane, Rohith Vaidyanathan, Srinath Srinivasa, Santosh Kumar Upadhyaya, and Srinivas Vivek. 2024. Consent Service Architecture for Policy-Based Consent Management in Data Trusts. In Proceedings of the 7th Joint International Conference on Data Science & Management of Data (11th ACM IKDD CODS and 29th COMAD) (CODS-COMAD '23). Association for Computing Machinery, New York, NY, USA, 155–163. https://doi.org/10.1145/3632410.3632415

STATES OF A CONNECTION



X NODES

1) After data access is granted via a connection, it is important to ensure that the resource also contains relevant meta-data that provide details of the consent, as well as enforce the terms of consent post sharing

2) A wrapper around a data element being shared that acts as a consent artifact

3) A smart contract enforcing post-conditions and sharing modalities.

4) X-nodes can be of different types based on sharing modalities: i-node, v-node, s-node

i-node: A type of X-node that represents primary ownership of a given data element

v-node: A type of X-node that represents an access privilege to a data element (akin to a pointer). The data element itself resides in the host locker and each access has to go through the data owner's consent primitives

s-node: A type of X-node that represents conferred or delegated ownership. The holder of an s-node has specific permissions on data element which is also available locally (unlike v-node) and acts as the owner of the data element for specific activities

X-NODES AND RESOURCE SERVER

1) In the overall architecture, X-nodes are meta-data containing information about consent, post-conditions and denote ownership capacity. These are exchanged between lockers.

2) However, the actual data resource (say degree.pdf), is present in a resource server. The actual location information is present in the i-node.

3) The important distinction here, is that when we are performing data transactions, only the x-nodes are flowing between lockers and not the resource itself. When a DR makes a request for an artifact, the artifact flow is first resolved using lockers and connections, following which, a request is made from a locker to the resource service to make the resource available to the DR

REPRESENTATION OF A XNODE

X-node	function	essential fields	essential post-conditions
i-node	"information" node: represents primary location of resource	creator, primary_owner, current_owner, shadows_list, v-node_list, pointer_to_resource, provenance	transfer, confer, share, collateral, subset, download
v-node	"virtual" node: represents an access privilege to an i-node	creator, current_owner, pointer_to_original, validity, v-node_list, provenance	transfer, share, download
s-node	"shadow" node: represents a conferred or pledged ownership	creator, primary_owner, current_owner, pointer_to_original, shadows_list, v-node_list, pointer_to_resource, provenance	transfer, share, collateral, subset, download

Table 2: Essential fields of X-nodes

Primary Owner: Agent has full authority over the data resource, including the ability to control access, modify, share, or delete the data at their discretion.

Current Owner: Agent who can exercise executive authority given by primary owner.

Node_Id	Node_metadata	APD	Type	Validity
10	{ "resource_location": "file:2025/transcripts.pdf", "primary_owner":"University" "current_owner":null "terms":<post_conditions> }	University: Transcripts	INODE	2025-10-19 06:42:34
25	{ "node_pointer": "s_node_id_54", "terms":<post_conditions> }	Company: Job Portal	VNODE	2025-10-19 06:42:34
54	{ "node_pointer": "i_node_id_10", "resource_pointer": "file:2025/transcripts.pdf", "primary_owner": "university", "current_owner": "student" }	Student: Education Docs	SNODE	2025-10-19 06:42:34

HOW TO TRANSACT X-NODES?

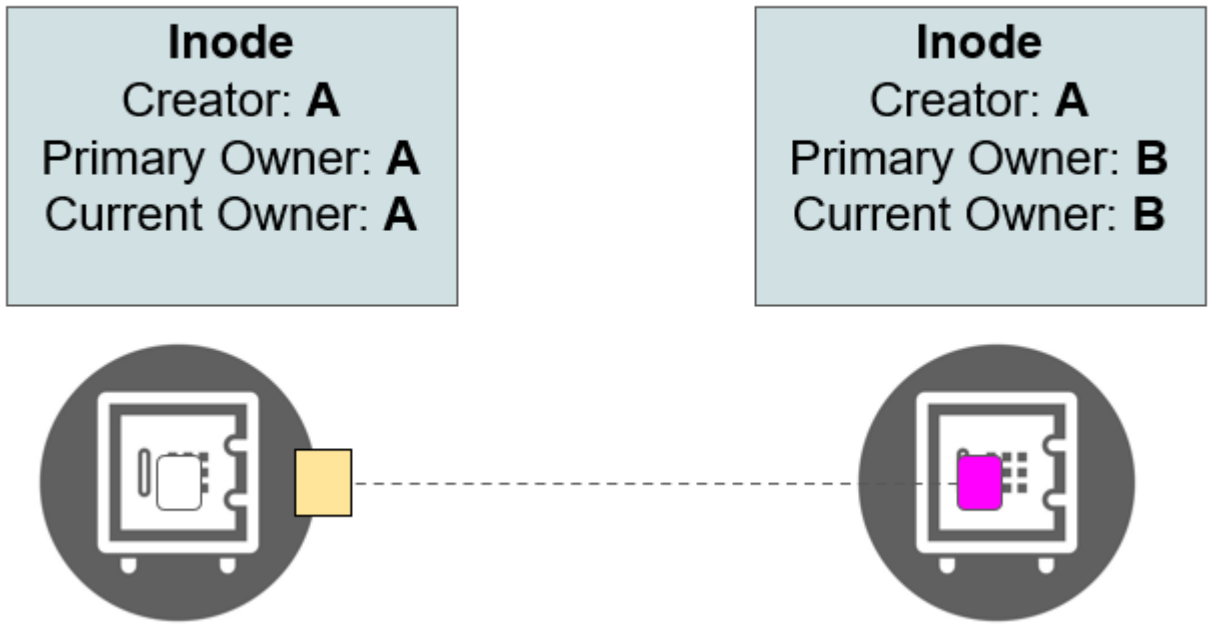
1) Transacting X-nodes between lockers, would mean modifying or sharing consent and ownership of the resource, as discussed previously.

2) Example: Selling a house: We *transfer* ownership to the new buyer by changing his name against the original property document. Thus, the previous owner loses access to this document.

SHARING OPERATORS - TRANSFER

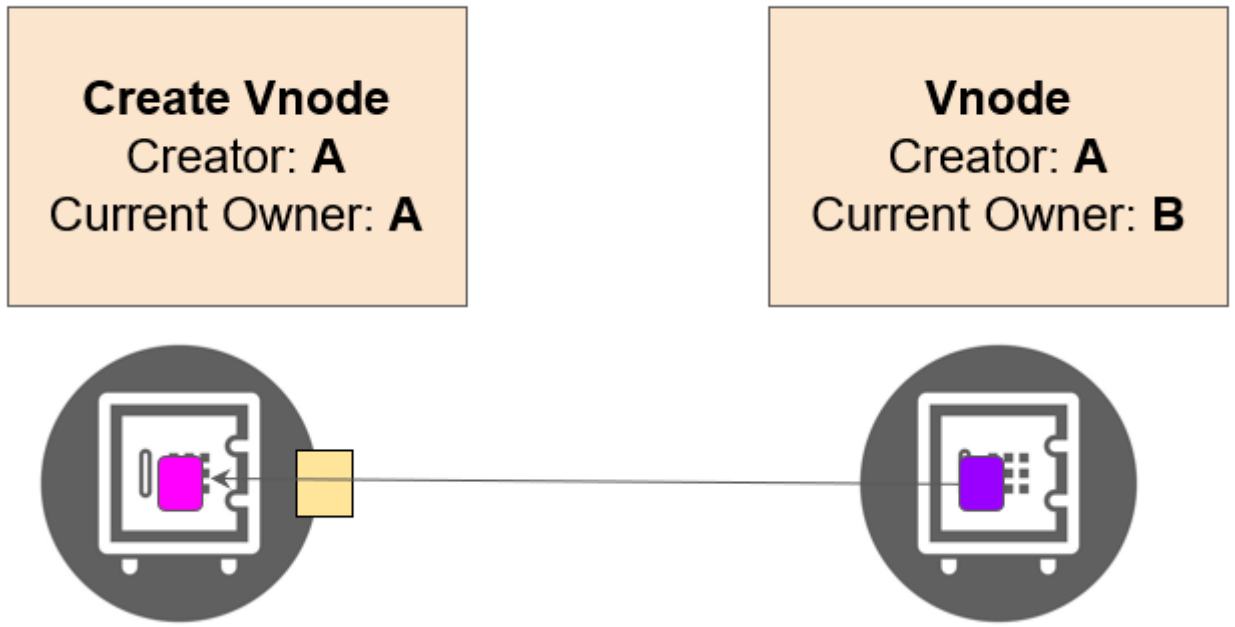
1) Ownership of the artifact is transferred in entirety from the Data Owner to the Data Requester

2) The i-node is removed from the former and given to the latter's locker.
3) Primary and current owner attributes are changed to the latter



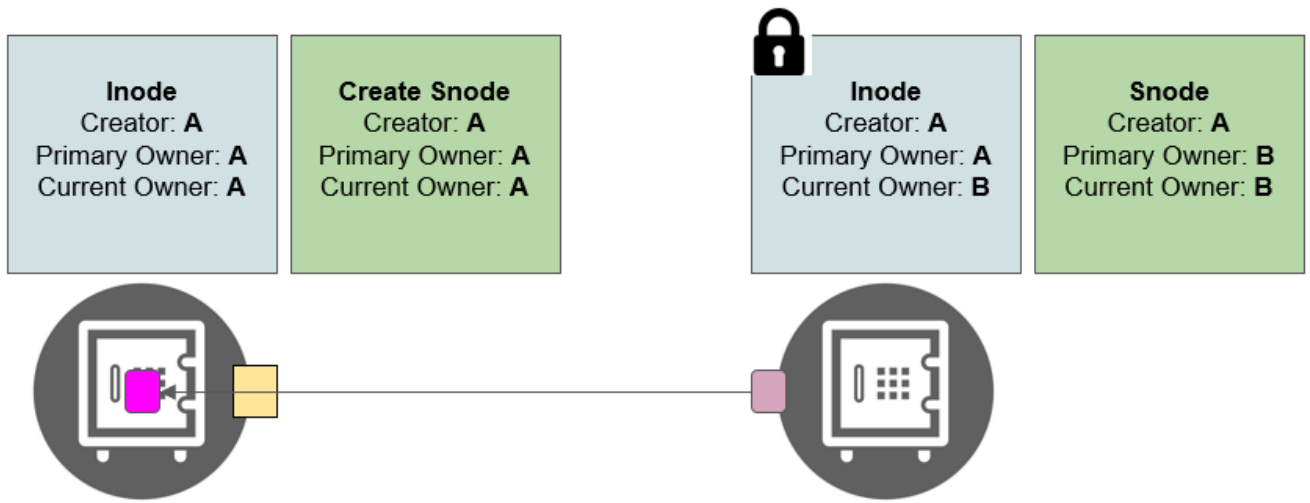
SHARING OPERATORS - SHARE

1) Ownership of the artifact does not change, only a consensual pathway is provided to access the artifact.
2) A v-node is created in the locker of the Data requester.
3) The vnode points to the location of the inode.



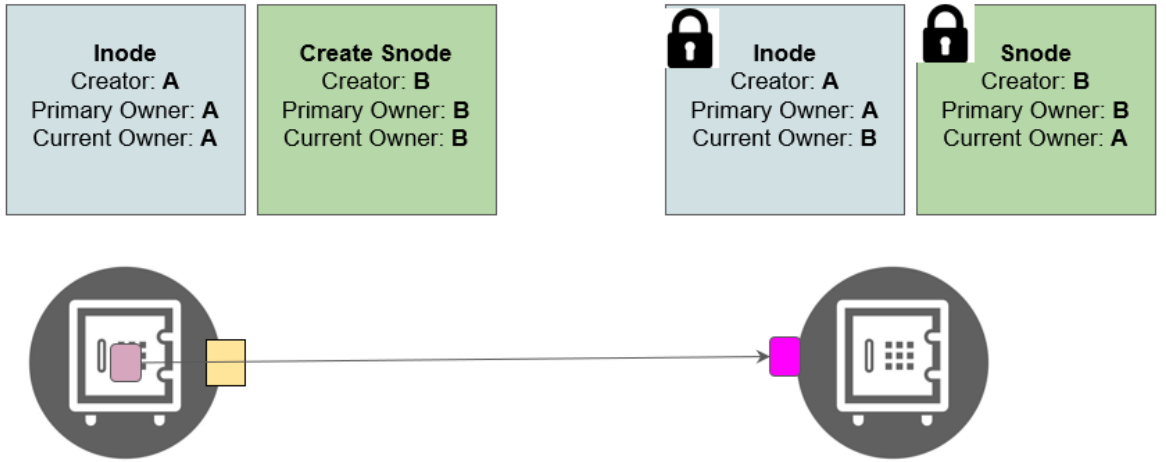
SHARING OPERATORS - CONFER

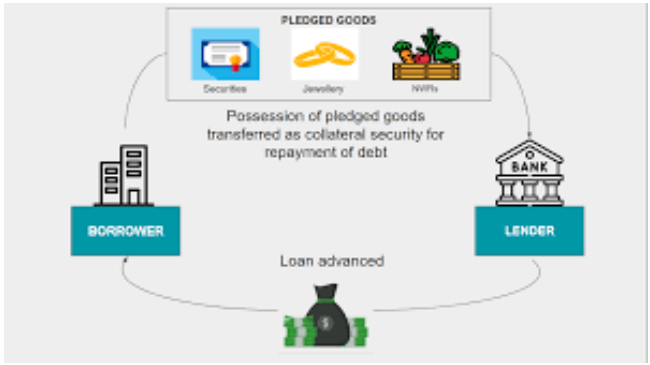
1) Data Requester is made a conferred/ delegated owner.
2) A s-node is created in the locker of the Data requester. He has immutable access to the artifact.
3) For verifying the legitimacy of conferred ownership, a link to the primary owner exists in the s-node
4) Primary owner – Data Owner
   Current Owner – Data Requester
5) Examples: Issuance of licenses, degrees etc.



SHARING OPERATORS - COLLATERAL

1) In this mode of sharing, data owner presents data element as a collateral to requester, obtaining only limited privileges, until some obligations are fulfilled. A s-node is created in the locker of the Data requester. He has immutable access to the artifact.
2) S-node is created with the Data Owner and the i-node is given to the Data Requester.
3) Primary owner is the Data Requester and the current owner is the Data Owner.
4) Example: Certain Colleges hold your original marks card, and will return it only after completion of your degree.





ARE SEQUENTIAL OPERATIONS POSSIBLE?

Take the example, of a student applying for a job. He would like to share access (SHARE) to the company, he is applying for.

SEQUENTIAL SHARING OPERATIONS

V-node that is created due to a SHARE operation, can be further subject to a SHARE (provided it is permitted by the post-conditions).

This creates yet another v-node pointing to the original v-node.

This can be used to create access tunnels where a resource can be accessed through a legitimate, consensual pathway comprising of several layers of consent.

V-node can be subject to a TRANSFER provided that it is permitted by the post-conditions created by the DO. When a v-node is transferred by a DR to another agent (say DR2), then the earlier DR loses the access pathway to the resource, which is now held by DR2

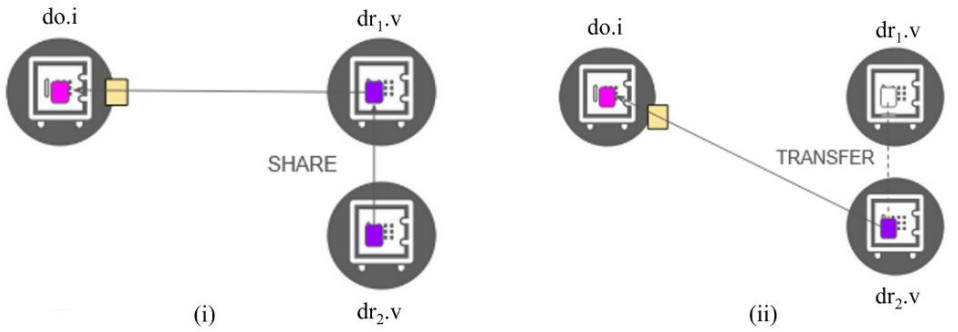


Figure 5: (i) An *access tunnel* established for origin of request (dr_2) to the ground of the request (do) after performing SHARE of a SHARE (ii) A v-node ($dr_1.v$) subject to TRANSFER from dr_1 to dr_2

SEQUENTIAL SHARING USING S-NODES

1) A s-node that is the result of a conferment can be further subject to SHARE, COLLATERAL or TRANSFER. In some cases, the primary owner may disallow TRANSFER as a post-condition at the time of conferment (as in the case of conferred degrees). A conferred s-node cannot be however, further conferred.

2) Locked artifacts that are a result of COLLATERAL operations, cannot be further transferred, conferred or pledged. However, SHARE operation is still defined on them (but may be prohibited by post-conditions), where access pathways can be established to locked x-nodes through v-nodes

CONCLUSION

1) The increasing number of Digital Public Infrastructure (DPI) implementations, handling and exchanging massive amounts of public data, has necessitated the need to handle consent at scale

2) When extending consent management over DPIs, we see that it is closely concerned with issues of individual or institutional autonomy, ownership, public well-being and national sovereignty

3) Different morphological forms of ownership also affect consent in different ways–which are captured by the concept of x-nodes

4) The proposed primitives help to indicate the ownership capacity of the one who is in custody of the artifact. The consent flow demonstrates a transition of ownership with the Data Owner legitimately delegating responsibility to the Data Requester, within the Data Trust