भारतीय मानक
Indian Standard

IS 18003 (Part 1) : 2020

यूनिफाइड डाटा एक्स्चेंज

भाग 1 आर्किटेक्चर

Unified Data Exchange

Part 1 Architecture

ICS 33.020, 35.020

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI-110002
www.bis.gov.in www.standardsbis.in

December 2020 **Price Group 8**

Smart Infrastructure Sectional Committee, LITD 28

FOREWORD

This Indian Standard was adopted by Bureau of Indian Standards, after the draft finalized by the Smart Infrastructure Sectional Committee, had been approved by the Electronics and Information Technology Division Council.

This standard is an Integral part of IS 18002 (under development). The system design principles, high level architecture and other aspects mentioned in this standard are derived from IS 18002 (Data layer Key guiding principles, Key characteristics, and Core functions). The traceability of this standard with the IS 18002 is provided in the Annex A.

The composition of the committee responsible for the formulation of this standard is given at Annex B.

INTRODUCTION

Data empowerment is a key aspect of any smart city implementation to harness maximum value from the enormous data cities generate. The current smart city implementations are unable to satisfy this need efficiently due to the proprietary and ad-hoc nature of the interfaces and their implementations. Hence, it is difficult to develop next generation AI/ML based applications for providing new solutions and services at scale, using the existing frameworks. The Data Exchange as discussed in this document aims to address this gap, by creating an architecture (Part 1) and interface specifications (Part 2) for interconnecting various IT systems of different government departments as well as external organizations**.**

The data exchange will provide three key services:

a) A catalogue service which will host a catalogue of meta-information about the various data sets, with information about the custodian of the data, data model for the data, the API endpoints, API methods etc.

b) One or more authorization services that will enable a data custodian (one who is responsible for the data) to regulate access to their data sets.

c) One or more resource access services which will allow a standardized way to access resources.

Security and privacy will be incorporated by design in this architecture. This architecture should simplify the life of the data custodian as well as the application developer.

The data exchange architecture will enable new applications to emerge that can take advantage of data from different IT Systems, to provide novel services. For example, a Women's safety index can calculate the live safety index of any street, combining data from smart streetlights, video analytics from traffic cameras, data from police databases along with analysis of land use. Such an index can be used by trip planning apps to allow for determining safe routes or used by the city or police to plan on patrolling.

By defining the architecture and specifying the interfaces and data models, the data exchange architecture standards will enable a whole new ecosystem of application developers to provide new, data driven, solutions and services. Additionally, adopting the data exchange architecture nationally, will enable economies of scale for the developers and will allow the same applications to run across the country. For data custodians – the data exchange architecture will allow a simple way to expose, provide consent, audit and track their data usage.

Indian Standard

UNIFIED DATA EXCHANGE

PART 1 ARCHITECTURE

1 SCOPE

1.1 This Indian Standard (Part 1) describes the architecture for the data exchange, interfaces of data exchange components and the use cases that are enabled in this ecosystem. It also describes the responsibilities of various stakeholders, their interactions with other stakeholders in the system, and the respective consequences of those interactions.

1.2 This Standard (Part 1) also describes the high level architecture of the following three main components of the data exchange services:

a) Catalogue service that provides APIs to manage meta-information about resources;

b) Authorization service, that manages authorization to access the resources; and

c) Resource access service, that provides a standardized way to access resources.

1.3 A more detailed specification and the API definitions for the data exchange architecture is described in part 2.

2 REFERENCES

The standards given below contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of these standards.

2.1 Normative References

The following referenced documents are necessary for the application of the present document.

[1] IETF RFC 2818: "HTTP Over TLS".

[2] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[3] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[4] IETF RFC 6749: The OAuth 2.0 Authorization Framework.

[5] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[6] IETF RFC 7232: "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests".

[7] IETF RFC 7946: "The Geo JSON Format".

[8] IETF RFC 8259: "The Java Script Object Notation (JSON) Data Interchange Format".

[9] IS 7900 : 2007: "Data elements and interchange formats — Information interchange — Representation of dates and times".

[10] ISO/IEC 19464 Information technology — Advanced Message Queuing Protocol (AMQP) v1.0 specification.

[11] IS/ISO/IEC 29100 : 2011 (en) Information technology — Security techniques — Privacy framework.

[12] OASIS : MQTT 5.0, OASIS Standard.

[13] Open Geospatial Consortium Inc. OGC 06-103r4: "OpenGIS® Implementation Standard for Geographic information-Simple feature access — Part 1: Common architecture".

[14] TRADE/CEFACT/2005/24 Recommendation No. 20 - Units of Measure used in International Trade.

3 TERMINOLOGY AND DEFINITIONS

For the purpose of this standard, the following definitions shall apply:

a) The key terminologies use consolas font type and dark cornflower blue 3 color encoding; and

b) The lower Camel Case is used in attribute naming. For nouns, UpperCamelCase is used.

3.1 Definitions

3.1.1 *Provider*

Provider is a **legal entity**. Human (possibly delegated by an organization), organization or an organizational role that has responsibility to provide authorization to use resources.

3.1.2 *Resource Server*

Resource server is a **service**. Serves resources to authorized Apps or Consumers.

3.1.3 *Consumer*

Consumer is a legal entity. Human or organization or an organizational role that consumes a resource via a web or mobile App. Autonomous systems may also act as a Consumer on behalf of a legal entity.

3.1.4 *App*

App is an application. Software (like a mobile app, web app, device app or server app), that uses resources to provide a service to the consumer.

3.1.5 *Provider App*

Provider App is an Application. An App that enables a provider to manage the meta-data and access control in the data exchange, for the resources they are responsible for.

3.1.6 *Data Exchange*

Data exchange is a service. Hosts and manages meta-data about resources and interfaces to manage authorization for accessing the resources.

3.1.7 *Consent*

Provider's freely given, specific and informed agreement to the accessing and processing of specific resources in their responsibility.

3.1.8 *Certificate Authority*

An entity which provides digital identities to participants of DX in the form of digital certificates.

3.1.9 *Personally Identifiable Information*

Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

NOTE — To entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

3.1.10 *PII Principal*

Natural person to whom the personally identifiable information (PII) relates

NOTE — To entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

3.1.11 *Authorization Token*

A machine-readable token that allows a consumer to get access to a provider's data. The authorization token is requested by a consumer for a set of resources, and is generated by an authorization service after running consent rules of a provider. The authorization token is to be presented to a resource server by a consumer while requesting for data. All authorization tokens shall have a valid expiration time.

3.1.12 *Catalogue*

A registry of meta-data about the resources in the data exchange available for consumption.

3.1.13 *Resource Item*

An entry in the catalogue that describes the meta-information of the resource that is hosted in an associated resource server.

3.1.14 *DX Authorization Service*

Authorization service of the data exchange.

3.1.15 *DX Catalogue Service*

Catalogue service of the data exchange.

3.1.16 *DX Adaptor*

Adapter service in front of a non-DX compliant resource server.

3.1.17 *DX Administrator*

DX administrator is a legal entity. Responsible for administering, managing and running the data exchange.

Abbreviations

Abbreviation	Definition
DX	Data Exchange
XML	eXtensible Markup Language
JSON	Javascript Object Notation
API	Application Programming Interface
PII	Personally Identifiable Information
CA	Certificate Authority
RS	Resource Server
AS	Authorization Service
TLS	Transport Level Security
CSR	Certificate Signing Request
CCA	Controller of Certifying Authorities

4 DATA EXCHANGE ARCHITECTURE

The data exchange (DX) is a set of services that enables consumption of resources (like data) by a consumer from one or more resource servers, based on explicit consent obtained from the provider of the resources.

4.1 System Design Principles

The architecture and design described in this Standard is based on the following principles:

a) *Technology Agnostic* — A system is said to be technology agnostic if its design is neutral to applications, programming languages, and platforms. The aim of DX is to be technology agnostic to provide seamless and secure flow of electronic data between different stakeholders.

b) *Reliability and Scaling* — Reliability is the probability of failure-free software operation for a specified period of time in a specified environment. DX systems shall be designed in a way that failure of one system should affect other systems minimally. Systems must also be designed to recover quickly from failures. The design should also allow for scaling individual systems when necessary.

c) *Privacy by Design* — Privacy by design is an approach where privacy is taken into account in the design and engineering aspects from early on. The data exchange implementation defines the data sharing mechanisms, based on Electronic Consent and results in a non-repudiable audit trail. The provider of the data resources controls the consent to access the resources. Hence, the provider shall ensure that PII of PII principals are dealt with as per the laws of the land [b.1, b.2]. The data exchange will also maintain the privacy of consumers and all other actors who interact with the exchange based on international standards [11].

d) *Security by Design* — Secure by design indicates that a software system has been designed from the ground up to be secure. The software and systems in the DX shall be secure by design. There shall be end-to-end security of data (PKI, Digital Certificates, tamper detection) and it shall be network agnostic and data centric.

e) *Consumer Centric* — Consumer experience and ease of use are critical to successfully deliver various services in an ecosystem. The DX should take into account the various stakeholder responsibilities and mechanisms to simplify interactions and ease the access to data and services for consumers.

f) *Consent Driven* — A consent-driven architecture is one where data is shared with a data consumer only if the data provider explicitly provides consent. In such a system, data providers must be provided with enough information about the consumer to make the consent decision. Mechanisms for dynamic discovery, empowerment of the provider in accordance with the consent architecture proposed in [b.2] shall be incorporated to enhance trust and ensure data privacy.

g) *Open APIs for Interoperability* — Systems should have standardized programmatic interfaces (Open APIs) for sharing and accessing digital resources easily. The data exchange specification shall define standard APIs to promote interoperability and deliver services that are designed to work with any device, form factor or network.

h) *Transparency through Data* — Transparency in city operations can be achieved through access to Open Data [b.3]. Access to such open data will enable high-quality analytics, accurate fraud detection, shorter cycles for system improvement and, most importantly, high responsiveness to consumer's needs. The DX shall allow cities to adopt this model of transparency by providing options to host Open Data through Open APIs.

4.2 Entities and their Responsibilities

Table 1 outlines the roles and responsibilities of the various entities involved in the data exchange ecosystem.

Table 1 Entities and their Responsibilities

(*Clauses* 4.2 *and* 4.3)

Entity	Responsibilities
a) Provider	1 Manages DX catalogue entries for resources owned. 2 Provides data for resources owned. 3 Manages access control list to authorize consumers.
b) Consumer	1 Request consent if needed for accessing secured data-set from appropriate provider. 2 Secure access token received to prevent any misuse.
c) Data Exchange	Hosts and manages meta-data about resources and interfaces to manage authorization for accessing the resources.
d) Resource Server	Serves provider's resources to authorized clients.
e) App	Consumer's application, that consumes resources on behalf of consumers.
f) Authorization Service	Provides authorization tokens to consumers of a DX if the consumers are authorized to. It also validates an Authorization token, when requested by a resource service.
g) Certificate Authority	Provides digital certificates. Their trust can be traced to the root certificate authorities.
h) Provider App	Helper application used by providers to manage interactions with the data exchange.
j) App Developer	An organisation or an individual developing applications that consumes, produces or manages resources.
k) Data Exchange Provider	Operates the data exchange.

4.3 High Level Architecture

The data exchange (DX) architecture consists of entities described in Table 1. The entities interact using interfaces as shown in Fig. 1.

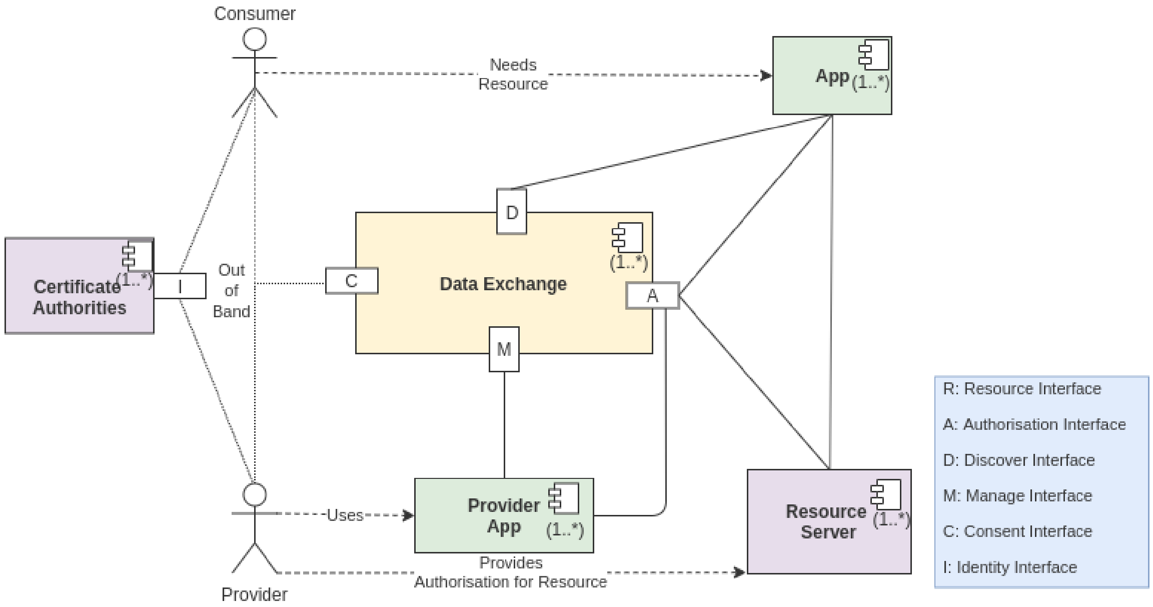

FIG. 1 DATA EXCHANGE ARCHITECTURE

The data exchange comprises the following interfaces:

a) Resource interface;

b) Authorization interface;

c) Discover interface;

d) Manage interface;

e) Consent interface; and

f) Identity interface.

Resources, managed by a provider, are hosted on one or more resource servers, and are made available for consumption to entities via a description of its meta-information (like its format, provider, etc.), through a catalogue in the data exchange. The catalogue is both human readable as well as machine-understandable.

The provider registers and manages the meta-data of its resources and their associated access control policies via the management interface of the data exchange. The provider **may** use a helper application, like the provider App. The meta-data of each resource should help an app developer to ease the consumption of resources in order to create useful applications for consumers.

The App can register with the data exchange to get notified about any changes to the meta-data of the resources of interest to the consumer. The App obtains consent to consume the resources via the authorization interface by obtaining an authorization token.

Any request to a provider's resource by a consumer App will be checked against the existing access control policies. If no decision can be made, the data exchange **may** coordinate between the provider and the consumer to complete a consent transaction and generate the authorization token. The authorization token will be logged by the system to ensure auditability of the consent flows. The coordination between the provider and consumer is done outside the scope of this specification and can be built using any of the available messaging technologies like SMS/OTP/EMAIL etc. The data licensing terms and conditions will also be outside the scope of this specification. However, reference to license **can** be provided in the meta-data for the resource.

In order to provide for a better consumer experience, the App seveloper **may** also enter into a resource licensing agreement with the provider. In this case, the consumer can be shielded from having to get consent separately, as long as the App developer and the App adhere to the licensing terms and conditions of the provider.

The set of interfaces for this data exchange architecture are listed in Table 2.

Table 2 Data Exchange Interfaces and Functionalities

(*Clause* 4.3)

Interface	Functionality	Remarks
Manage	Create, update, delete, list, search and view the items in the catalogue. Create, update, delete and view access control policies. List and view information about consumers.	Interface for the provider to manage the resource meta-info and access-control policies.
Discover	List, search, view and count items in the catalogue	Search can use complex queries and filters involving geo, time and other attributes
Authorization	Request, grant, revoke, introspect access tokens for resources.	Federated authorization flows.
Resource	Get latest data, search for resources, get status, get counts, subscribe, update subscription, unsubscribe. Playback of live and archived media streams, download media files. Stop, Pause and Stop playback. GIS resources access. Service resources access.	Retrieve latest data and search for resources using complex queries and filters. Search can be on Geo, time and other attributes.
Identity	Get identities	This interface connects with external identity management systems. Defining this will be out of scope for this standard currently.
Consent	Get consent from provider	This interface enables consumers to get providers information to request consent for accessing protected, private or confidential data. Since it involves interactions with Humans - it is not defined as part of this standard currently. SMS/Phone/Mail etc can be used. Note that in case of embedded PII, provider has responsibility to get consent from PII principals.

These interfaces are specified in detail in Part 2 of this standard.

There are no deployment restrictions imposed by the DX. Data exchange using the said architecture and the associated interface specifications, can be deployed in multiple different ways and DX does not favour or impose any specific deployment model.

4.4 Establishing Identities of Participants

The identities of the providers, App developers **shall** be established via X.509 certificates. The identity of consumers **may** also be established via ID tokens (Open ID connect, SAML 2.0 or industry standards). The provisioning and management of these certificates or Tokens will be outside the scope of this standard.

4.5 Data Exchange Services

The two main services provided by the data exchange (DX) are the catalogue service, that allows management and search of meta-data about resources, and the Authorization service that manages authorization to access the resources. These are described in detail in **4.5.1** and **4.5.2**.

4.5.1 *Catalogue Service*

On a high level the DX catalogue service enables the following:

a) *Discovery of Data Resources* — By providing various search mechanisms to discover the resources of interest.

   1) For example, geo-based search, text search on meta-information, attribute search with a given value etc.

b) *Ease of Consumption of Data* — By providing links to data models objects that describe various attributes of the given resource. This facilitates data interoperability and easy integration into various applications.

   1) Data-models **may** contain description of data types, units, value constraints, text descriptions, semantic context etc. for the data associated with a given resource.

c) *Semantic Modelling of Meta-information — By* providing semantic contexts for the attributes describing meta-information which leads to improved machine readability, interpretability, operational interoperability and enables vocabulary reuse from other data-model stores and taxonomies.

d) *Ease of Access to Data from a Resource* — By providing formal descriptions of how to access the data from a resource.

1) For example, API objects to describe REST based resources etc.

e) *Feedback Mechanism* — The catalogue shall provide a feedback mechanism for consumers of the data to rate and review the resource.

At the core, DX catalogue is a store of *meta-information* associated with the data assets/resources available with the data exchange. A meta-information object may be related to another meta-information object by providing explicit references to one another. Further, using concepts of linked-data[1)], semantic grounding may be provided for the attributes contained in the meta-information objects. The DX catalogue, built on top of the meta-information store, provides powerful search capabilities to discover resources of interest and their associated meta-information (for example, data models, api objects etc.). Additionally, the DX catalogue provides services to build and maintain the meta-information store in a consistent and collaborative fashion.

The meta-information in catalog shall be in machine-understandable format and **may** use open standards such as JSON-LD. The meta-information for a resource shall support reviews from consumers.

4.5.1.1 *Catalogue interface*

DX catalogue exposes services via a set of APIs built on top of the meta-information store. The APIs can be broadly categorised into two sets:

a) Search APIs to discover resources of interest. The catalogue supports the following search methods:

1) Geo-spatial search: Discover items in a given geo-spatial bound (applicable to items containing geo-spatial attributes);

2) Attribute search: Discover items with a given value for a given attribute; and

3) Text search: Discover items that contain matching words in a set of textual attributes (for example, text descriptions etc.).

b) Management APIs to create, update and delete items.

Further details of catalogue are provided in Part 2 of this specification. In particular the following catalogue aspects will be described in detail:

1) API Specifications; and

2) Representational aspects of meta-information objects: various types of objects and relationships between the objects, representation formats etc.

4.5.2 *Authorization Service*

4.5.2.1 *Goals and non-goals*

The main goal of the DX framework is to enable seamless sharing of resources while respecting ownership, privacy and compliance requirements. DX achieves this by defining a set of open standards for authorization, data classification, and policy authoring, and providing sample implementations according to these standards. The standards enable data providers and application developers to target a consistent set of APIs for authoring policies and accessing data across smart city platforms. When DX is used for sharing sensitive or PII, the standards ensure that PII principals retain control over data shared on the platform in accordance with the strongest privacy regulations.

The authorization service in DX is designed to reduce barriers for adoption. In particular, resource providers should be able to start sharing resources with authorized entities with minimal effort. Towards this end, DX will support mechanisms for plugging existing non-DX complaint resource and authorization servers into the DX ecosystem with simple extensions. The authorization service also supports a simple-to-understand data classification framework and policy authoring tools to help providers migrate to the DX framework.

The following aspects of resource sharing are out of scope of DX authorization service.

a) *Data Collection Mechanisms* — DX does not mandate how data is collected from edge devices and transferred to the resource server.

b) *Enforcement of Policy Mechanisms* — DX does not currently provide mechanisms for enforcing policies such as data retention. Data providers are expected to enforce policies through other means such as legal agreements. However, the DX framework shall support technologies such as trusted execution environments for policy enforcement at the time of data use.

c) *Compliance Requirements* — DX does not mandate that policies meet specific compliance requirements. It is the responsibility of the provider to ensure that the policy they define meets the required compliance requirements and laws. For example, DX does not mandate that a data provider only share information for which consent for sharing has been obtained.

d) *Information Leakage* — DX is not responsible for any leakage of information that may occur through sharing. Providers are expected to ensure that data is appropriately sanitized, for example, via anonymization.

e) It is outside the scope of DX to prescribe what the consumer ought to do with the received data,

[1)] https://www.w3.org/DesignIssues/LinkedData post the retention period set by the provider. It is expected that the consumer disposes of the data in accordance with the policy requirements set by the provider, any legal agreement entered into with the provider or any regulatory framework governing the data. [DR(1)]

f) DX is not responsible for the correctness of the data sharing policy rules of a provider. The providers shall ensure that their data policy rules match their organization's policies; and go through the review process, be vetted by concerned parties, and tested before applying.

4.5.2.2 *Functionalities*

The authorization service in DX **shall** support the following functionalities:

a) *Authentication* — A DX authorization service shall allow users to authenticate themselves and participate in data exchange with valid X.509 certificates.

b) *Resource Access Policy Management* — A registered resource provider should be able to register resources to be shared in the DX catalog service and enable the DX authorization server to authorize access to resources on behalf of the provider. Resources **may** be associated with scopes and policies that define the set of resource attributes a consumer can access.

c) *Resource Access Authorization* — A consumer application uses the information in the catalog to request access from a DX compliant resource server. The resource server in conjunction with the DX authorization server determines if the consumer should be granted data access. Once authorization has been obtained, subsequent requests for data access **may** be serviced entirely by the resource server.

4.5.2.3 *Actors in the authorization flow*

The main actors of the architecture are:

a) *Provider* — Data providers setup access control policies for resources they are serving via the policy interface exposed by the DX authorization server.

b) *Consumer Application* — The consumer application requests access to data from the resource server on behalf of the consumer. Consumers are expected to obtain X.509 certificates from a certificate authority trusted by the DX. The trusted CAs shall include certificate authorities licensed by Controller of Certifying Authorities, Ministry of Electronics and Information Technology, Government of India. The DX may also accept certificates from other trusted CAs.

c) *Resource Server* — The resource server hosts resources (data and services). It grants access to resources after validating tokens issued by the DX authorization server.

d) *DX Adapter* — The DX Adapter is an optional entity that sits in front of a non-DX compliant resource server. It handles resource access requests from the consumer application on behalf of the resource server.

e) *DX Authorization Server (DX AS)* — The DX authorization server is a DX/UMA 2.0 complaint auth server that can be configured to control access to resources on behalf of the provider. It exposes endpoints needed for managing policies, permissions and tokens.

5 SECURITY AND PRIVACY

This section elaborates on the prerequisites for maintaining security and privacy in the data exchange architecture. It details the means by which authentication, consent and identity is established. The manner in which Authorization policies are to be created by the provider is also detailed. Privacy requirements in particular shall adhere to the laws of the land [b.1].

5.1 Security Requirements

a) All participants **shall** use TLS [1][3] to connect with DX.

b) The DX **shall** accept client side TLS certificates issued by a list of trusted CAs.

c) The list of trusted CAs **shall** be decided by the DX and **shall** be communicated to DX participants.

d) Security Techniques and best practices specified in [b.4][b.5][b.6][b.7][b.8][b.9][b.10][b.11][b.12][b.13][b.14][b.15] **may** be followed.

e) Scheduled and on-demand security updates from the cloud to edge devices shall be possible.

5.2 Privacy Requirements

a) All resource-items **shall** be tagged as either "public", "protected", "private", or "confidential".

b) The protocols used to access resources **shall** always use secure protocols based on TLS.

c) The authorization token **shall** be sent through a secure and encrypted channel.

d) The authorization token **shall** contain the authorization server and consumer ID for which the token belongs to. For example:

1) auth.iudx.org.in/user@domain.com/1802a84d157ff4d113150aeca8bdacee

e) If the request requires access to PII data, then along with the token, additional consent may be required from data principals in the form of OTP or biometrics.

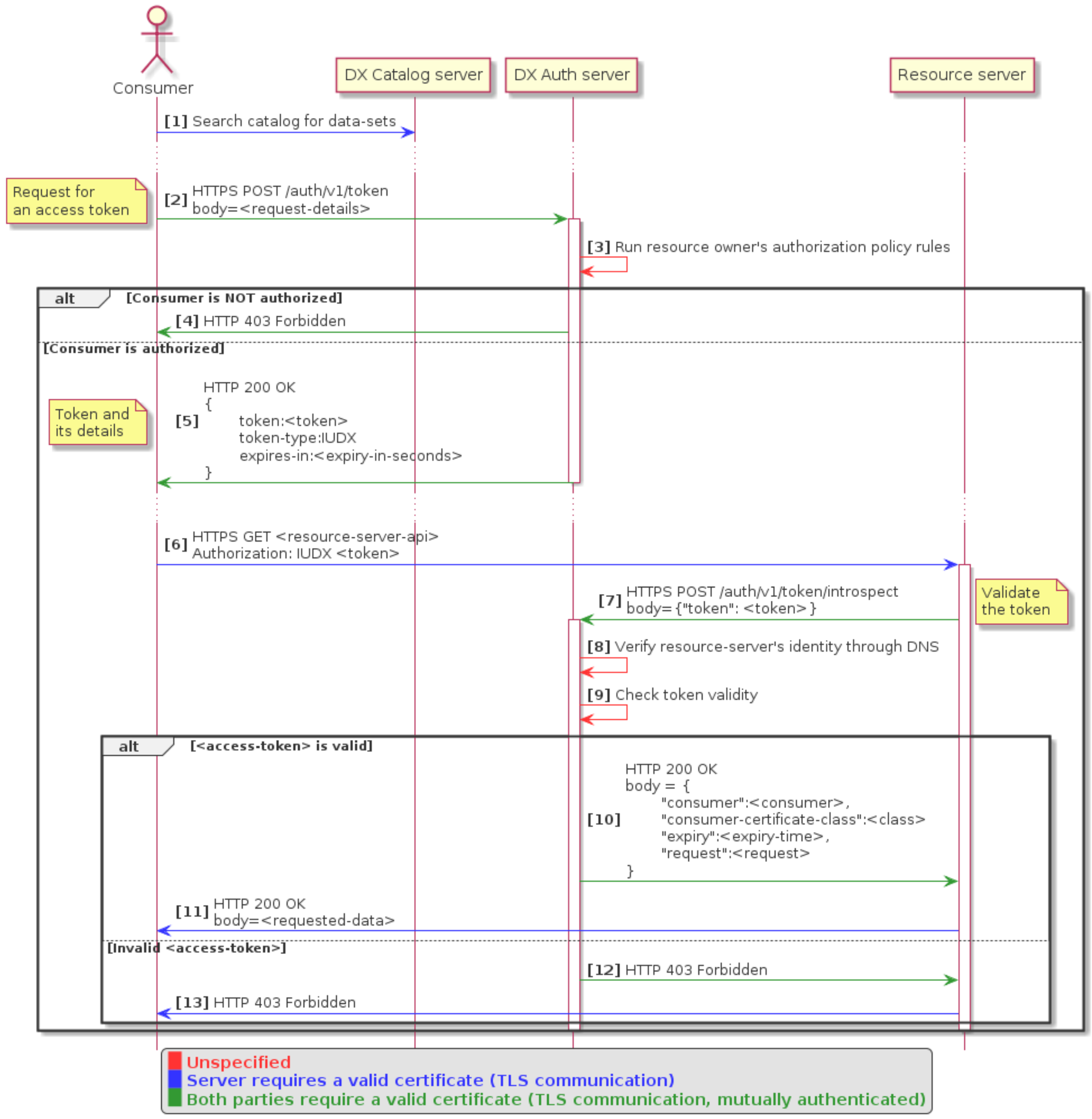
Consumer
DX Catalog server
DX Auth server
Resource server
[1] Search catalog for data-sets
Request for an access token
[2] HTTPS POST /auth/v1/token body=<request-details>
[3] Run resource owner's authorization policy rules
alt
[Consumer is NOT authorized]
[4] HTTP 403 Forbidden
[Consumer is authorized]
Token and its details
[5] HTTP 200 OK { token:<token> token-type:IUDX expires-in:<expiry-in-seconds> }
[6] HTTPS GET <resource-server-api> Authorization: IUDX <token>
[7] HTTPS POST /auth/v1/token/introspect body={"token": <token>}
Validate the token
[8] Verify resource-server's identity through DNS
[9] Check token validity
alt
[<access-token> is valid]
[10] HTTP 200 OK body = { "consumer":<consumer>, "consumer-certificate-class":<class> "expiry":<expiry-time>, "request":<request> }
[11] HTTP 200 OK body=<requested-data>
[Invalid <access-token>]
[12] HTTP 403 Forbidden
[13] HTTP 403 Forbidden
🟥 Unspecified
🟦 Server requires a valid certificate (TLS communication)
🟩 Both parties require a valid certificate (TLS communication, mutually authenticated)

FIG. 2 AUTHORIZATION FLOW

5.3 Authentication and Consent

a) All Providers **shall** use certificates from DX-CA or trusted certificate authorities to connect with DX.

b) The certificates **shall** be validated by authorization service and be checked against certificate revocation lists or OCSP.

c) All providers **shall** be able to manage the access control list of their resources using their valid digital certificates.

d) Catalog security:

1) Only people with proper authorization **shall** be able to create, update and delete entries in the catalog.

2) The entries in the catalog are linked to the DN of a user's certificate. Thus, only the original owner **shall** be able to modify their own entry.

e) Consent history: Consent history data is to be considered private and is only available to the Provider of the resource. Consent history **can** be made available to providers for audit purposes.

5.4 Authorization Policies

DX **shall** enable providers to associate a policy with every resource-item in the catalog. The policy **should** govern who has access to the resource described by the item and how entities with access **should** handle storage of resource's data.

A policy ***P*** is a pair of the form (***C***, ***A***), where:

a) ***C*** defines the set of consumers that are authorized for resource access. ***C*** may be defined in a policy language, such as XACML or Aperture. A consumer is any entity, such as an individual, organization, an organizational role, or a trusted execution environment that has been issued a certificate or token by a trusted CA.

b) ***A*** is a list of attribute-value pairs which defines requirements on consumers who have access to data.

The policy framework does not capture requirements around ownership of data. However, further additions to the list of attributes or attribute values **may** be made while maintaining backward compatibility.

Standard Operating Procedures (SOPs) may be defined for data usage, access rights and enforcement of integrity. And blockchain based technologies may be used to ensure data integrity. Also, business continuity procedures may be laid down as per ISO 22301.

5.4.1 *Policy Labels*

In order to simplify the process of authoring policies, the standard defines a set of policy labels that capture commonly used policy specifications as shown in Table 4.

Table 3 Authorization Policy Attributes and Values.

(*Clause* 5.4)

Attribute key	Description	Possible Values
Authorization protocol and policy	Specifies protocol that a consumer shall use to request access from a resource server	None, OAuth/UMA, OAuth/UMA + XACML Policy, Token/DX + Aperture policy language
Data locality	Specifies requirements on where a consumer is allowed to store data after getting access	Country, State, Organization (Service-based access), None
Data retention	Specifies requirements on how long consumers may retain data	Fixed period, Up to a certain event or date, None
Data storage	Specifies in what form a consumer may store data	Encrypted (using adequately protected keys), Encrypted at rest and in transit (using keys owned by data owner), Any
Data usage	Specifies requirements on the purpose for which data is used.	Privacy preserving computation, Anonymization, Computation certified by a third party, Any
Data audit	Specifies audit requirements on data that the consumer shall satisfy	Audit accesses along with time and duration of access, None

Table 4 List of Policy Labels

(*Clause* 5.4.1)

Labels → Meaning | v	Public	Protected	Private	Confidential
Nature of data	Information which can be made available to the public. It shall not contain any personally identifiable information	May contain anonymized information	May contain personally identifiable information	May contain personally identifiable information and/or other data that is confidential within an organization
Authorization protocol and policy	None	Requires authorization using DX/UMA	Requires authorization using DX/UMA	Requires authorization using DX/UMA
Consent	None	Requires consent of Provider	Requires consent of Provider and owners	Requires consent of Providers and owners
Data locality	None	None	Configurable or as per regulatory framework	Only service based access
Data retention	None	None	Configurable or as per regulatory framework	NA
Data storage	Any	Any	Encrypted	NA
Data usage	Any	License	Licensed with legal framework	Licensed with legal framework
Data audit	None	Random audit	Regular audit	Regular audit
Data Monetization	Not to be monetized	Provider's decision	Provider's decision	Provider's decision

Classification of data shall be the responsibility of the data provider and needs strict regulation wherever deemed necessary.

5.4.2 *Identity*

The identities of the providers and consumers accessing private data must be clearly established using digital certificates, whereas consumers accessing public data could be anonymous.

Identity of providers/consumers of data in DX is through:

a) Certificates; and

b) Tokens.

However Individuals, app developers, or employees of an organization who wish to access protected private, or confidential data shall require a valid certificate.

DX shall accept TLS connections using certificates from any licensed CA in India (certified by the CCA).

5.4.2.1 A DX **may** issue certificates to users based on their email IDs. A DX **may** host a certificate authority (CA) which can grant certificates to:

a) Resource servers;

b) Individuals/App developers;

c) Organizations;

d) Data officers of an organization; and

e) Employees of an organization.

A simple email based scheme **may** be chosen to issue certificates; for example:

Individuals and App developers **can** send a certificate signing request (CSR) as an attachment in an email to the DX Certificate Authority with subject "*Certificate request*". The CA will validate the CSR and will respond back with a certificate.

Organizations **can** send a certificate signing request (CSR) as an attachment in an email from their organization domain to DX Certificate Authority. The CA will validate the CSR and will respond back with a certificate. The certificate provided to an organization can only be used to grant certificates to employees of the organization. Thus, the domain name of the organization shall match with the e-mail of the employee to whom the certificate is granted.

For organizations to be able to request certificates from CA, they **shall** register themselves with CA (this **may** be through an online form). All registered organizations' domain names **shall** be added to a white-list; and DX **shall** only accept certificate requests from organizations in the white-list.

5.4.2.2 Organizations while generating a certificate **may** add more details about the employee, such as organization, organization unit, first name, last name, role of the employee, state, city, etc.

Employees of an organization **may** send a certificate signing request (CSR) as an attachment in an email to DX Certificate Authority. The organization that will act as a sub-CA or a registration-authority will validate the CSR and will respond back with a certificate. The scripts/tools to grant certificates **may** be provided by the DX to organizations.

The DX Certificate Authority **shall** issue 5 classes of certificates:

a) Class 1: Which **shall** be issued to resource servers for validating tokens.

b) Class 2: Which **shall** be issued to individuals or employees of an organization (which are registered and whitelisted with the DX). This certificate is expected to be used to access protected data.

c) Class 3: Which can be issued to employees and data-officers of an organization (which are registered and whitelisted with the DX). Such employees **shall** have access rights to upload and manage resource-items in the catalogue of the DX. This certificate **shall** be used to create/manage catalog items.

d) Class 4: Which is to be issued to trusted employees of an organization (which are registered and whitelisted with the DX). This certificate is expected to be used to access protected and private data.

e) Class 5: Which is to be issued to trusted employees of an organization (which are registered and whitelisted with the DX). This certificate is expected to be used to access protected, private, and confidential data.

5.5 Audit Considerations

All interfaces **shall** make statistics available and log all events to allow audit of interactions.

5.6 Reliability Considerations

The systems shall be designed to be highly available, scalable using a distributed architecture for vertical and horizontal scale, and high on performance where:

a) Reliability is defined as the ability of a device or a system to perform its intended function under given conditions of use for a specified period of time or number of cycles.

b) Availability is defined as the property of being accessible and usable upon demand by an authorized entity.

c) Scalability is defined as the property of a system to handle a growing amount of work/load by adding resources to the system.

The public API status page **may** be provided by the authorization service provider, catalogue service provider and the resource server that reports the status of each API (along with other open data like average response time, latency, etc). Furthermore, these **may** also implement the heartbeat API for reporting their system uptime in real-time.

The various failure scenarios that shall be handled are as follows:

5.6.1 *Failure to Notify Provider*

In this scenario, when the AS or RS is not able to notify the provider on the status of the consent flow or data flow, a mechanism has to be put in place to notify the provider at a later stage. This can be achieved by reinitiating the notification message to the provider or by providing the provider an option to check the status through an application, or by providing a list of all consent flows and data flows (with status) in the application.

5.6.2 *Response from AS does not Reach the Consumer*

In this scenario, when the response sent by AS does not reach the Consumer, the latter should have a mechanism provided by AS to initiate a request to know the status of the consent flows.

5.6.3 *Response from Catalogue Service does not Reach Consumer*

In this scenario, when the response sent by catalogue service does not reach the consumer, the consumer should have a mechanism provided by catalogue service to initiate a request to know the status of catalogue services.

5.6.4 *RS is not Available to Consumer*

In this scenario, when RS is not available to consumer, consumer **may** have a mechanism to re-initiate the request to RS.

6 INTERACTION SCENARIOS

The minimal set of interaction scenarios supported by the data exchange ecosystem is indicated in Fig. 3. Details for each follows.

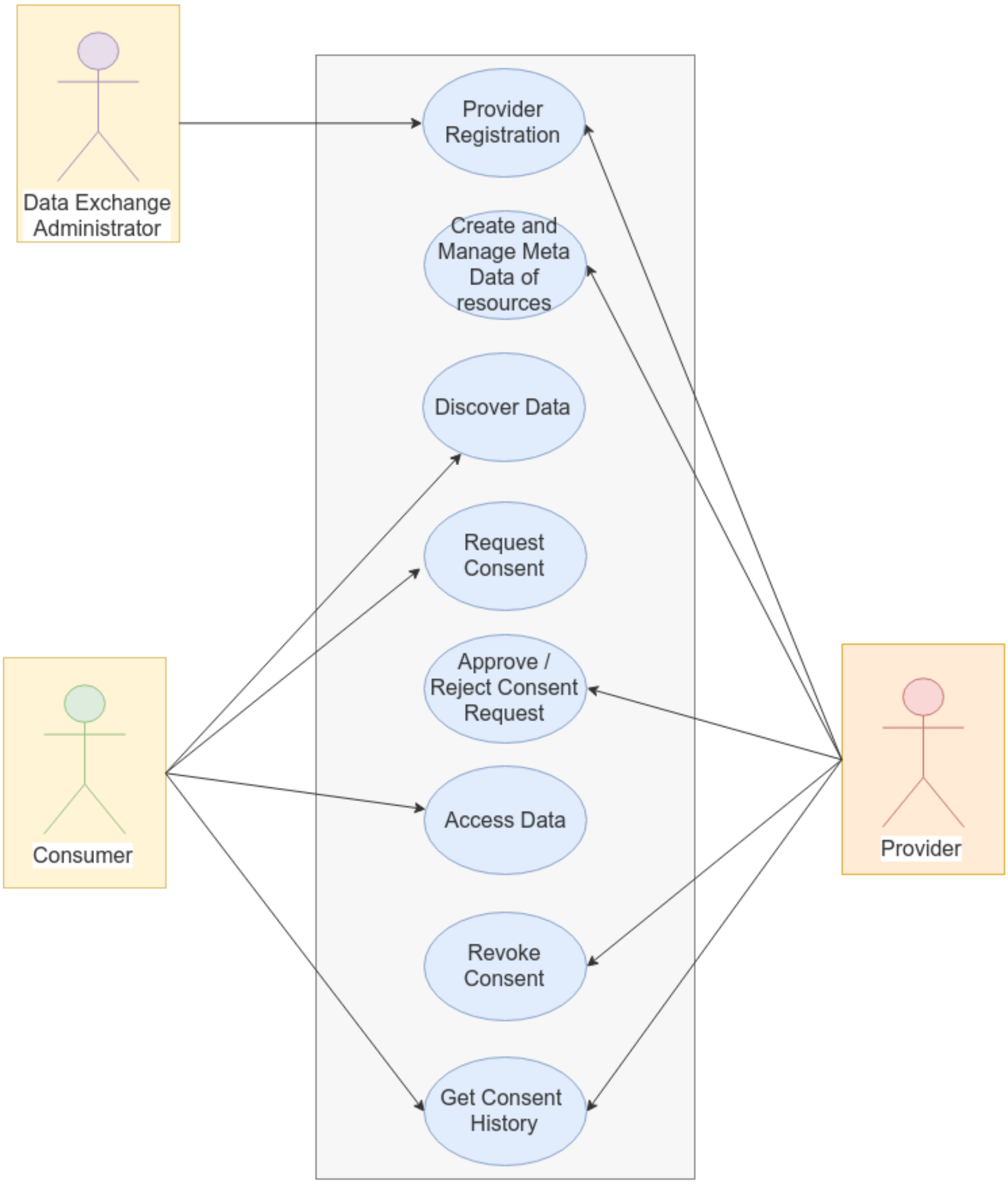

FIG. 3 BASIC INTERACTION SCENARIOS

6.1 Provider Registration

The provider needs to obtain a certificate from the CA to establish identity. An example workflow is given as follows:

6.2 Create and Manage Metadata of Resources

In this use case, a Provider is requesting the authorization service to allow access to use the catalogue. Once approved, the provider can create or update an entry in the catalogue.

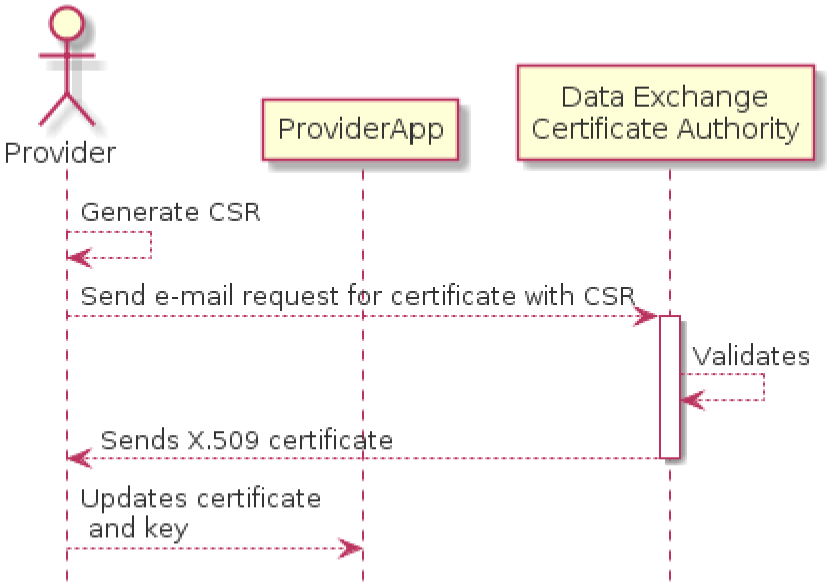
Provider
ProviderApp
Data Exchange Certificate Authority
Generate CSR
Send e-mail request for certificate with CSR
Validates
Sends X.509 certificate
Updates certificate and key

FIG. 4 PROVIDER REGISTRATION FLOW

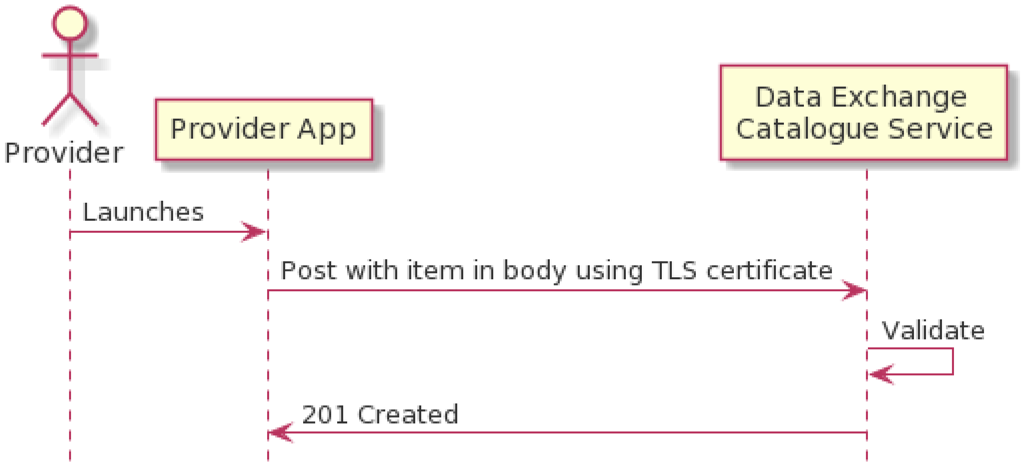
Provider
Provider App
Data Exchange Catalogue Service
Launches
Post with item in body using TLS certificate
Validate
201 Created

FIG. 5 RESOURCE PROVIDER CREATING AN ITEM IN THE CATALOGUE

Summary	The use case allows Providers to update the catalogue
Pre-condition	- A valid certificate provided by a trusted CA
Actor	Provider
Post-condition	An approval is provided to perform the requested operation

If a resource is not public, then the Provider can request an Authorization Service to set policies for data access.

Summary	The use case allows Providers to set policies for their resources
Pre-condition	- A valid certificate provided by a trusted CA
Actor	Provider
Post-condition	A policy is set for the provider’s resources.

6.3 Discover Data

In this use case, a consumer is using the search APIs of the catalogue service to find interested entities. Once the entities are identified, a consumer using consumer App can request for consent and access their data.

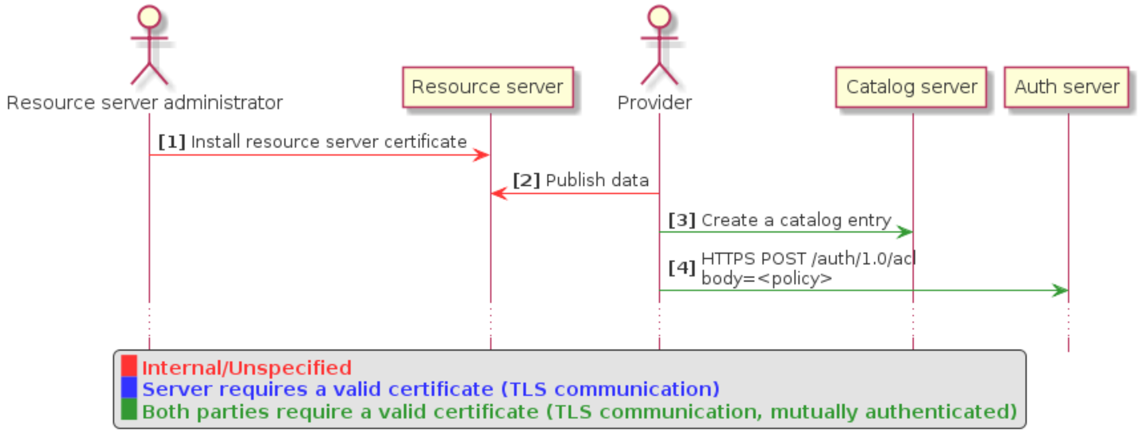
Resource server administrator
Resource server
Provider
Catalog server
Auth server
[1] Install resource server certificate
[2] Publish data
[3] Create a catalog entry
[4] HTTPS POST /auth/1.0/acl body=<policy>
🟥 Internal/Unspecified
🟦 Server requires a valid certificate (TLS communication)
🟩 Both parties require a valid certificate (TLS communication, mutually authenticated)

FIG. 6 SETTING UP A PERMISSIONS FOR A RESOURCE BY THE PROVIDER

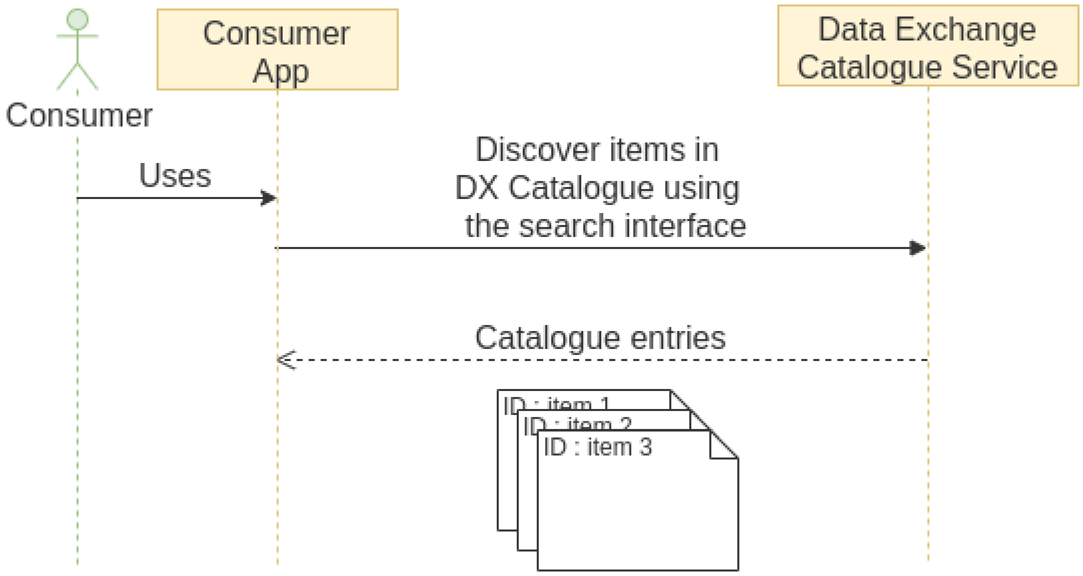
Consumer
Consumer App
Data Exchange Catalogue Service
Uses
Discover items in DX Catalogue using the search interface
Catalogue entries
ID : item 1
ID : item 2
ID : item 3

FIG. 7 CONSUMER DISCOVERING DATA

Summary	This use case allows consumers to search the catalogue using customer app
Pre-condition	–
Actor	Consumer
Post-condition	A list of search hits are sent to the consumer app

6.4 Request Consent and Access Data

A consumer application can request access to data from an DX compliant resource server using any one of the supported APIs. If requested data does not require authorization that is, does not have an authorization policy, or the request contains a valid access token, then the resource server serves the request after token validation.

If data requires authorization and the request does not contain a token, the resource server initiates authorization following a DX/UMA 2.0 compliant protocol. The protocol supports a subset of UMA 2.0 workflows:

a) Accept policies specified in a policy language.

b) Support identities based on X.509 certificates issued by DX CA (as described above)

c) Accept claims based on X.509 certificates issued by a set of trusted CAs

d) No support interactive claims gathering. All claims shall be pushed.

e) Include a reference to the policy object in access tokens issued

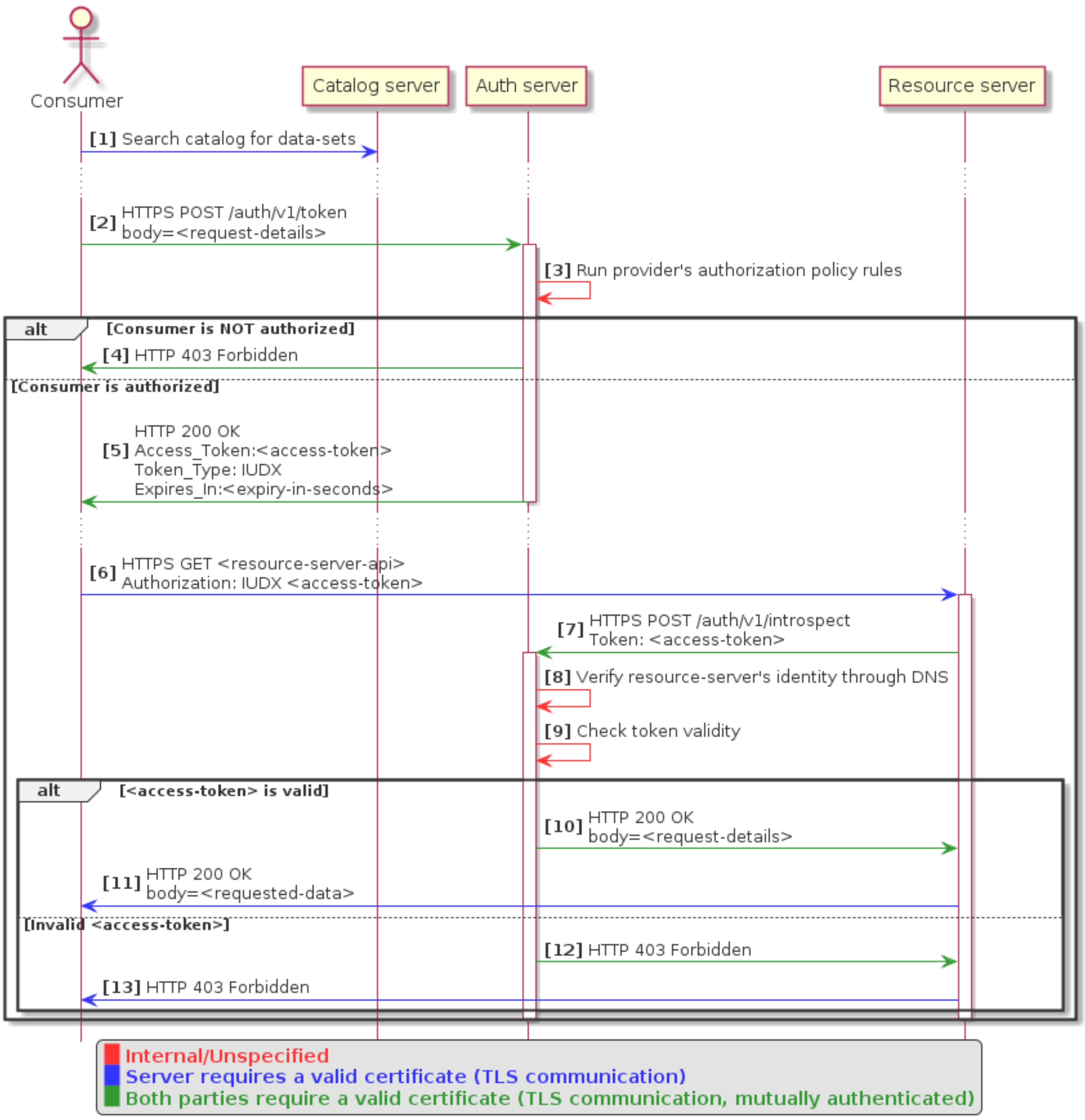
Consumer
Catalog server
Auth server
Resource server
[1] Search catalog for data-sets
[2] HTTPS POST /auth/v1/token
body=<request-details>
[3] Run provider's authorization policy rules
alt [Consumer is NOT authorized]
[4] HTTP 403 Forbidden
[Consumer is authorized]
[5] HTTP 200 OK
Access_Token:<access-token>
Token_Type: IUDX
Expires_In:<expiry-in-seconds>
[6] HTTPS GET <resource-server-api>
Authorization: IUDX <access-token>
[7] HTTPS POST /auth/v1/introspect
Token: <access-token>
[8] Verify resource-server's identity through DNS
[9] Check token validity
alt [<access-token> is valid]
[10] HTTP 200 OK
body=<request-details>
[11] HTTP 200 OK
body=<requested-data>
[Invalid <access-token>]
[12] HTTP 403 Forbidden
[13] HTTP 403 Forbidden
🟥 Internal/Unspecified
🟦 Server requires a valid certificate (TLS communication)
🟩 Both parties require a valid certificate (TLS communication, mutually authenticated)

FIG. 8 CONSUMER REQUESTING ACCESS TO A RESOURCE

Summary	This use case allows the Consumer to access the requested data
Pre-condition	• A valid X.509 certificate issued by a DX compliant CA
Actor	Consumer Application
Post-condition	The requested data is provided to the Consumer

6.5 Revoke Consent

A provider **shall** be able to revoke access to a particular resource by calling the/revoke API.

Summary	This use case allows the Provider to revoke access to data
Pre-condition	• A valid X.509 certificate issued by a DX compliant CA
Actor	Provider Application
Post-condition	The consumer is no longer able to access the resource

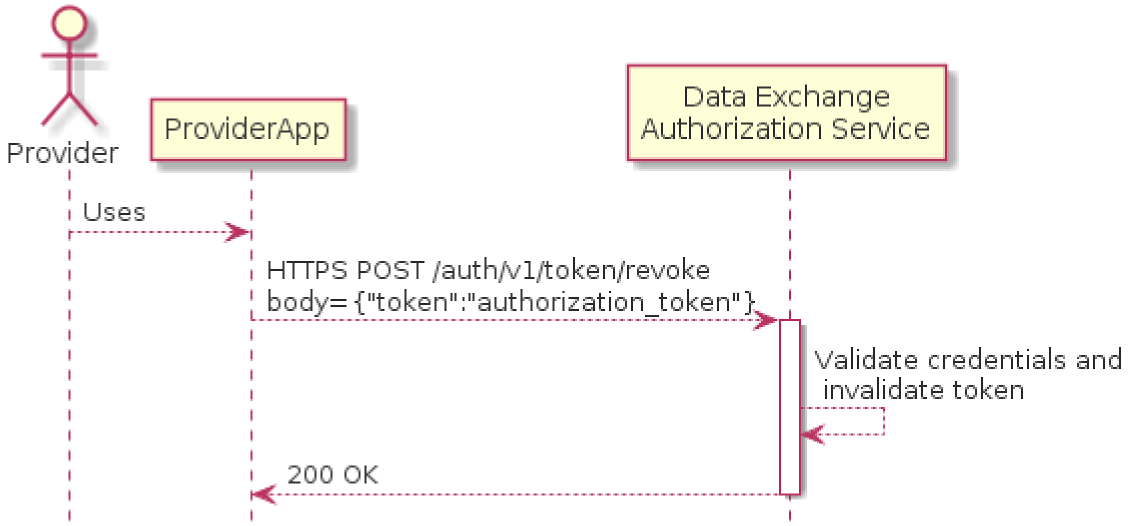
Provider
ProviderApp
Data Exchange Authorization Service
Uses
HTTPS POST /auth/v1/token/revoke
body={"token":"authorization_token"}
Validate credentials and
invalidate token
200 OK

FIG. 9 REVOKING CONSENT FLOW

ANNEX A

(*Foreword*)

TRACEABILITY WITH DATA LAYER REFERENCE ARCHITECTURE

The below table shows the traceability of this document with IS 18002 data layer reference architecture (Under Development). The sections detailed in this document expand on the initial definitions and concepts in the data layer document.

Section in this Document	Section in the DL Document
3: Terminology and Definitions	• Terminology and Definitions
4.1: System Design Principles 4.2: Entities and their responsibilities	• Data Layer-Key Guiding Principles • Data Layer-Key Characteristics
4.3: High Level Architecture	• Data Layer Core Functions (Architecture diagram)
4.4: Entities and their responsibilities	• Data Layer-Key Guiding Principles (Accessibility)
4.5: Data Exchange Services	• Data Layer-Core Functions • Unified Data Layer Architecture and Components-Data Exchange API • Data Exchange
5: Security and Privacy	• Unified Data Layer Architecture and Components - Data Governance
6: Interaction Scenarios	• Data Exchange-Data APIs

ANNEX B

(*Foreword*)

COMMITTEE COMPOSITION

Smart infrastructure Sectional Committee, LITD 28

Organization	*Representative(s)*
Indian Institute of Science, Bengaluru	Prof Bharadwaj Amrutur (***Chairman***)
Amravati Smart City Development Corporation Limited, Mumbai	Shri Siddharth Ganesh
ARM, Noida	Shri Kumaar Guhan
Centre for Development of Telematics, New Delhi	Shri Aurindam Bhattacharya Shrimati Anupama Chopra (*Alternate*)
Criterion Network Labs, Bengaluru	Shri Jayaprakash Kumar Shri Krishna Kumar Lohati (*Alternate*)
Cyan Connode Private Limited, Bengaluru	Shri Deepak Nimare Shri Manish Widhani (*Alternate*)
E-Goverments Foundation, Bengaluru	Shri Krishnakumar Thiagarajan
Ericsson India Private Limited, Gurugram	Shri Sendil Kumar Devar
ESRI, Noida	Shri Vijay kumar Shrimati Seema Joshi (*Alternate* I) Shri Rupesh Kumar (*Alternate* II)
European Project SESEI	Shri Dinesh Chand Sharma
Hawlett Packard Enterprise	Shri R. Devarajan
IEEE India, Bengaluru	Shri Srikanth Chandrasekaran Shri Munir Mohammed (*Alternate*)
India Smart Grid Forum, New Delhi	Shri Reji Kumar Pillai Shrimati Parul (*Alternate*)
Indian Institute of Science, Bengaluru	Shri Vasanth Rajaraman
Intel India Technology Private Limited, Bengaluru	Shri C. Subramanian Shri Anantha Narayanan (*Alternate* I) Shri Sidhartha Mohanty (*Alternate* II)
Ministry of Housing and Urban Affairs, New Delhi	Shri Kunal Kumar
MoHUA Smart Cities Handholding team	Shri Padam Vijay
Narnix Technolabs Private Limited, New Delhi	Shri N. Kishor Narang
National Smart Grid Mission, Ministry of Power, Gurugram	Shri Mr Arun Misra Shri Gyan Prakash (*Alternate* I) Shrimati Kumud Wadhwa (*Alternate* II)
PHYTEC Embedded Private Limited, Bengaluru	Shri B. Vallab Rao (Vasu)
Pune Smart City, Pune	Shri Manojit Bose
Qualcomm India Private Limited, Bengaluru	Dr Vinosh Babu James Dr Punit Rathod (*Alternate*)

Organization	*Representative(s)*
Renesas Electronics, Bengaluru	Ravindra Chaturvedi Saurabh Goswami (*Alternate*)
Schneider Electric's industrial software business-AVEVA, Mumbai	Shri Gourav Kumar Hada Shrimati Sangeeta Garg (*Alternate*)
Secure Meters Limited, Gurugram	Shri Uttam Kotdiya Shri Anil Mehta (*Alternate* I) Shri Puneet khurana (*Alternate* II) Shri Kaustubh Patil (*Alternate* III)
Shrama Technologies Private Limited	Shri Amarjeet Kumar
Siemens Limited, Mumbai	Shri Manoj Belgaonkar Shri Ravi Madipadga (*Alternate* I) Shri Pradeep Kapoor (*Alternate* II) Shri Vikram Gandotra (*Alternate* III)
Standardization Testing and Quality Certification (STQC)	Shrimati Lipika Kaushik
System Level Solutions (India) Private Limited, Anand	Shri Dipen Parmar Shri Foram Modi (*Alternate*)
Tata Consultancy Services Limited, Mumbai	Shri Ramesh Balaji Shri Debashis Mitra (*Alternate*)
Tejas Networks Limited, Bengaluru	Dr Kanwar Jit Singh
Telecommunication Engineering Center, Department of Telecommunications, New Delhi	Shri Rajeev Kumar Tyagi Shri Sushil Kumar (*Alternate* I) Shri Uttam Chand (*Alternate* II)
In Personal Capacity	Prof Suptendranath Sarbadhikari
BIS Director General	Shrimati Reena Garg, Scientist 'F' and Head (Electronics and IT) [Representing Director General (*Ex-officio*)]

Member secretary

Shri Manikandan K
Scientist 'D' (Electronics and IT), BIS

Panel involved in the preparation LITD 28/P12 Data Exchange Architecture

Organization	*Representative(s)*
Indian Institute of Science, Bengaluru	Prof Bharadwaj Amrutur (***Convener***)
Aikaan	Chetan Kumar
Bosch	Vivekanand K.
Indian Institute of Science, Bengaluru	Dr Abhay Sharma Anand S. V. R. Dr Arun Babu Bryan Robert Poorna Chandra Tejasvi Prof Bharadwaj Amrutur Rakshit Ramesh Vasanth Rajaraman
Intel India Pvt Ltd	Akshay Kadam Sidhartha Mohanty (*Alternate* I) Subramanian C. (*Alternate* II)
Microsoft Research	Dr Kapil Vaswani
Pune Smart City	Manojit Bose
HPE	R. Devarajan
SIRPI.io	Anand Lakshmanan
Tejas Networks	Dr K. J. Singh

BIBLIOGRAPHY

[b.1] The Personal Data Protection Bill 2019, Govt. of India, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[b.2] Electronic Consent Framework, Technical Specs v1.1, http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf

[b.3] National Data Sharing and Accessibility Policy 2012, Govt. of India, https://data.gov.in/sites/default/files/NDSAP.pdf

[b.4] ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements

[b.5] ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security controls

[b.6] ISO/IEC 27017, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[b.7] ISO/IEC 27018, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[b.8] ISO/IEC 27031, Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity

[b.9] ISO/IEC 27033 (all parts), Information technology – Security techniques – Network security

[b.10] ISO/IEC 27034 (all parts), Information technology – Security techniques – Application security

[b.11] ISO/IEC 27035 (all parts), Information technology – Security techniques – Information security incident management

[b.12] ISO/IEC 27040, Information technology – Security techniques – Storage security ISO/IEC 29100, Information technology – Security techniques – Privacy framework

[b.13] ISO/IEC29101, Information technology – Security techniques – Privacy architecture framework

[b.14] ISO/IEC 29134:2017, Information technology – Security techniques – Guidelines for privacy impact assessment

[b.15] ISO/IEC 29151, Information technology – Security techniques – Code of practice for personally identifiable information protection

[16] BACnet: BACnet — A Data Communication Protocol for Building Automation and Control Networks. http://www.bacnet.org/

[17] Brick: A uniform metadata schema for buildings. https://brickschema.org/

[18] Project Haystack: https://project-haystack.org/

[19] JSON-LD: https://json-ld.org/

[20] Business Continuity Planning: https://www.iso.org/standard/50038.html

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc No.: LITD 28 (14073).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices:		*Telephones*
Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110002	2323 7617 2323 3841
Eastern	: 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi KOLKATA 700054	2337 8499, 2337 8561 2337 8626, 2337 9120
Northern	: Plot No. 4-A, Sector 27-B, Madhya Marg CHANDIGARH 160019	265 0206 265 0290
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600113	2254 1216, 2254 1442 2254 2519, 2254 2315
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East) MUMBAI 400093	2832 9295, 2832 7858 2832 7891, 2832 7892

Branches : AHMEDABAD. BENGALURU. BHOPAL. BHUBANESHWAR. COIMBATORE. DEHRADUN. DURGAPUR. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. JAMMU. JAMSHEDPUR. KOCHI. LUCKNOW. NAGPUR. PARWANOO. PATNA. PUNE. RAIPUR. RAJKOT. VISAKHAPATNAM.

Published by BIS, New Delhi