Knodia

Cross-Border Federated Interoperability

EXECUTIVE SUMMARY

Get in touch — info@knodia.org

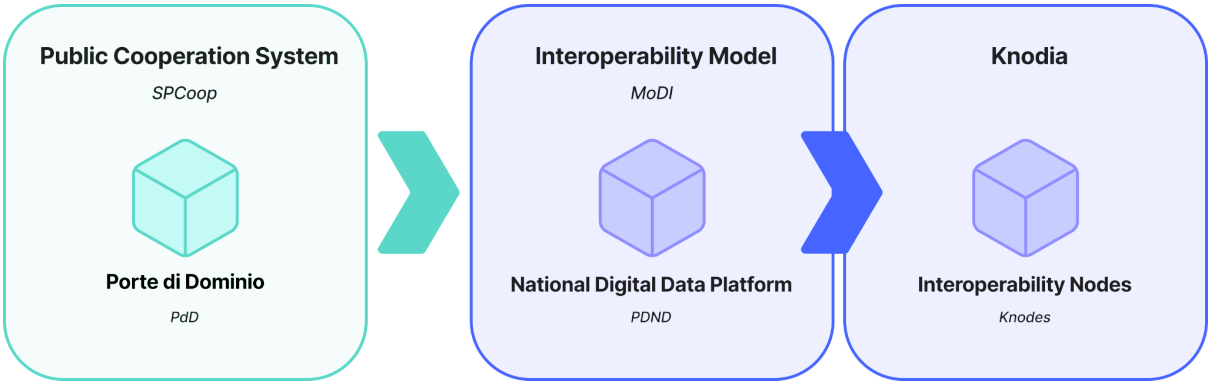
---

v1.0 15 January 2026

Knodia

This document describes the Italian proposal to the *Interoperable Europe Board* for the experimentation of *Knodia* within the interoperability regulatory sandboxes established by the *Interoperable Europe Act*. *Knodia* is a *cross-border federation* that manages authentication and authorization for interested organizations to enable data exchange on digital channels and the integration of cross-border digital services.

The Knodia proposal originates from the positive experience of the *National Digital Data Platform* (*PDND*) in Italy. The latter is the infrastructure for authentication and authorization of organizations – both public and private – within the *Interoperability Model* of Italian public administrations.



Knodia is intended to comply with the current European regulatory framework on interoperability and on the protection of personal data of natural persons.

The need for authentication and authorization

Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (in brief, the *Interoperable Europe Act*) identifies the *European Interoperability Framework* (*EIF*) as a set of guidelines and recommendations on legal, organizational, semantic, and technical interoperability, addressed to all entities falling within its scope.

The current version of the *EIF* is the one set out in Annex 2 to the *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (COM/2017/0134 final) regarding the European Interoperability Framework – Implementation Strategy*.

The objectives of the *EIF* are met by establishing a shared infrastructure of services and information sources that enables communication between the information systems of interested parties via application programming interfaces (APIs), as expressed in Recommendation 36 of the *EIF*.

In this scenario (regardless of the specific application domain that the interaction between interested parties involves), there is the need to authenticate and authorize access to APIs and ensure their usage in compliance with the regulatory framework regarding the protection of personal data of natural persons – primarily, *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (*GDPR*). This need aligns with the *interoperability agreements* between organizations in the provision of a European public service, mentioned in Recommendation 26 of the *EIF*.

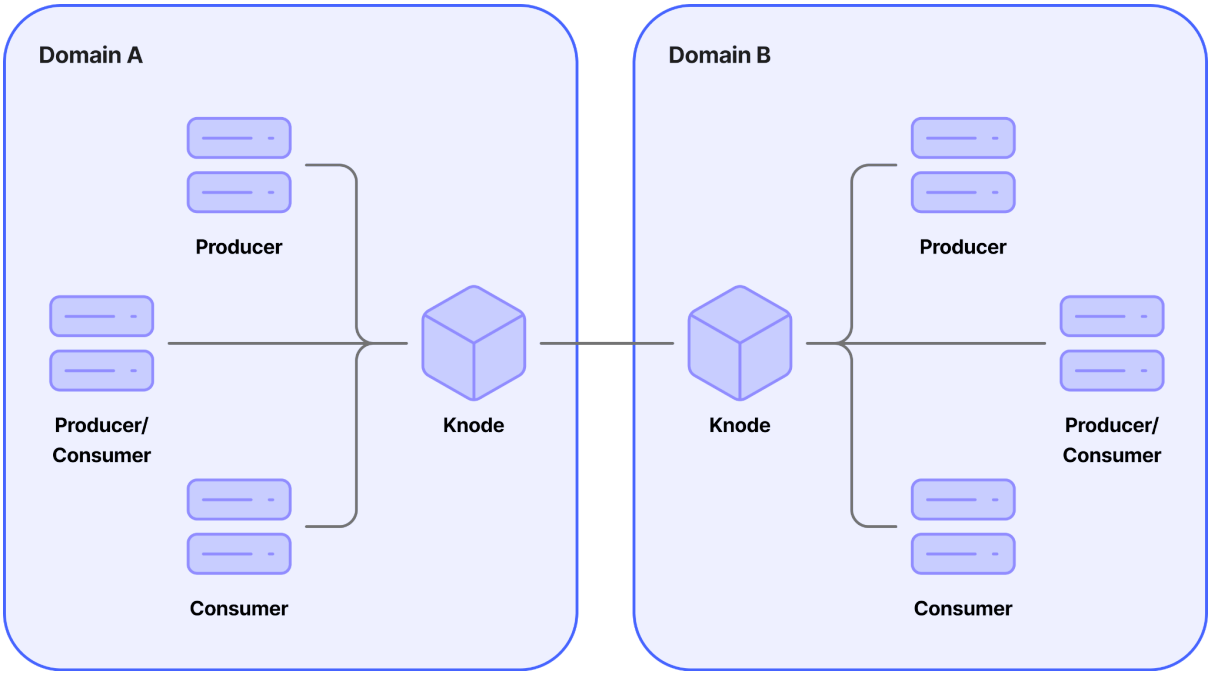
The definition of Knodia, which capitalizes on the Italian experience of the *PDND*, pursues the following objectives:

- Ensure the identification of organizations participating in the ecosystem (*Confederate Organizations*) and guarantee the assignment of *attributes* to them.
- Allow Confederate Organizations to make APIs available for access to data and services for which the organization itself is the authoritative source (*Producers*).
- Allow Producers to limit which Confederate Organizations can request access to their APIs based on those Organizations' attributes.
- Identify a process by which potential *Consumers* request access to APIs from Producers, adaptable to the regulatory frameworks of Member States where needed.
- Allow Consumers to declare, in compliance with the *GDPR* and any applicable Member State laws, the lawfulness of the processing of data they access via API.

Proposed solution

Within Knodia, cross-border data sharing and service integration are enabled through *Cross-Border E-Services*.

Organizations make Cross-Border E-Services available – hereinafter *produce* them – by defining an application programming interface (API) and the associated metadata that characterize it. This allows other interested organizations to use them – hereinafter *consume* them.



Knodia provides for the existence of the following actors:

- The Interoperability Nodes (hereinafter, *Knodes*), which are the managers responsible for identifying and managing each one a distinct set of Confederate Organizations, offering them the functionality needed to enable interaction with Confederate Organizations of other Knodes;
- The Confederate Organizations, which are the organizations that assume either or both roles of:
    - *Producers*, when they provide E-Services to other Confederate Organizations;
    - *Consumers*, when they consume the E-Services of the Producers.

Taken together, the Knodes, Producers, and Consumers constitute Knodia, which is based on trust established between the participating Knodes. Producers and Consumers are recognized as participants in Knodia and engage in cross-border interactions based on the information exchanged by the Knodes that have recognized them.

A consortium of the Knode managers (hereinafter the *Knodia Consortium*) is necessary to establish Knodia's governance. The appropriate venues shall evaluate whether this consortium can be implemented by the Interoperable Europe Board, as defined in Article 15 of the Interoperable Europe Act.

The Knodes equip themselves with the technological components required to join Knodia, in accordance with the requirements defined and shared by the Knodia Consortium. Producers and Consumers adopt the communication standards and protocols identified by Knodia to engage in cross-border interactions with each other and in machine-to-machine interactions with the Knodes.

In the following, where not ambiguous, the terms Knodes, Producers, and Consumers are used to indicate both the organizations and the technological components they implement to join Knodia.

E-Service consumption flow

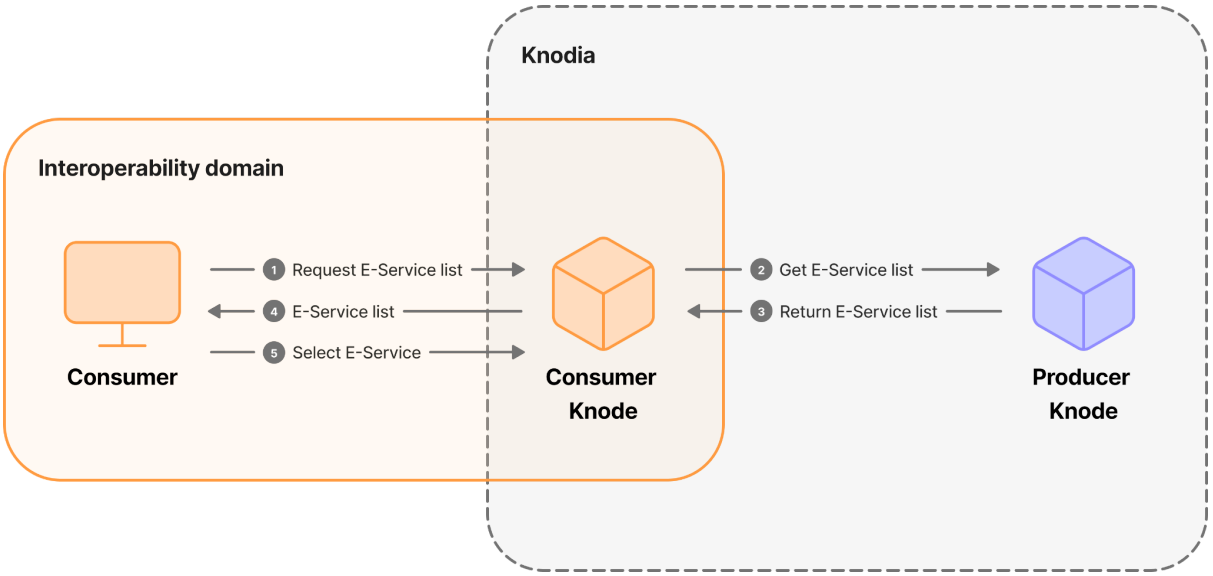
This section describes, at a high level, the actions that – given a Cross-Border E-Service published by a Producer on its Knode (hereinafter the *Producer Knode*) – allow a Consumer belonging to a different Knode (hereinafter the *Consumer Knode*) to access the E-Service.

E-Service publication

The Producer registers the Cross-Border E-Service on the Producer Knode to enable cross-border usage. This includes defining the consumption requirements, which are the characteristics (*Attributes*) that potential Consumers must satisfy to access the E-Service.

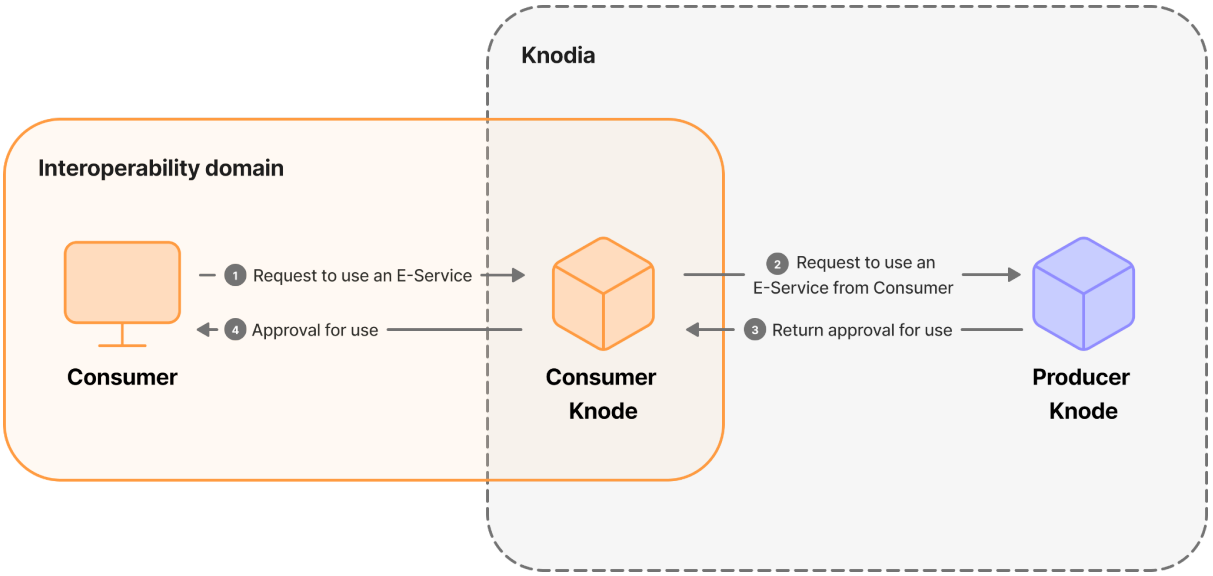
E-Service search

Potential Consumers who need to retrieve data or integrate services beyond their own Interoperability Domain can look through the Cross-Border E-Services offered by other Knodes. This is made possible by the interaction between Knodes. The Consumer identifies the E-Service of interest.



Agreement Request

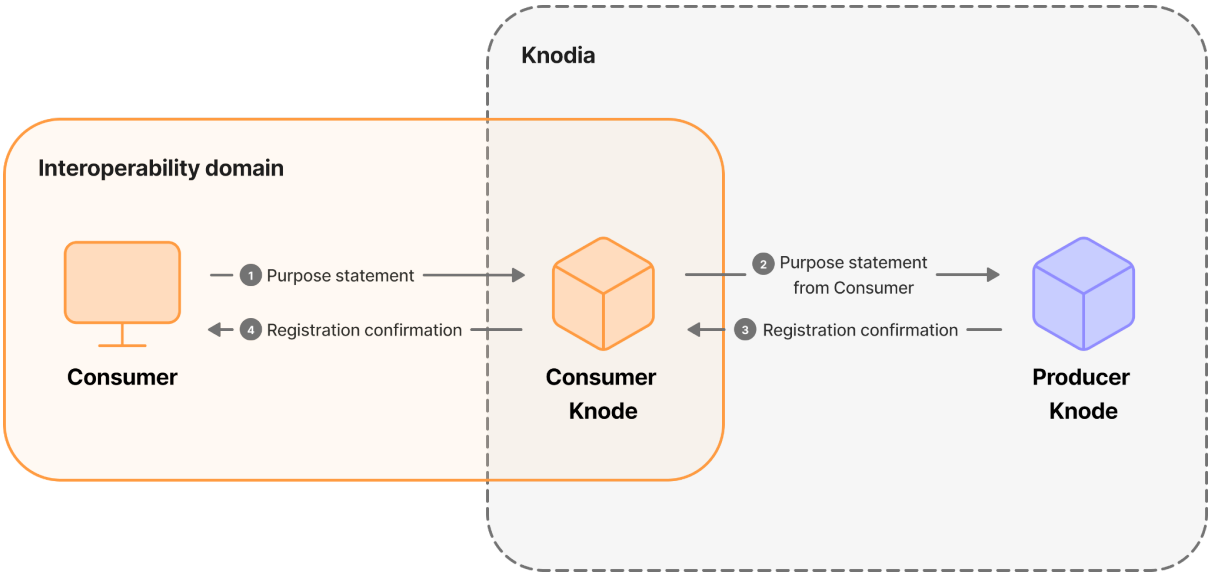
The potential Consumer can initiate an *Agreement Request* for the Cross-Border E-Service, provided it possesses the Attributes indicated by the Producer in the consumption requirements. To send the Agreement Request, the Consumer interacts directly with the Consumer Knode, which forwards the request to the Producer Knode.



The Producer Knode can request additional information from the Consumer to implement the national regulatory framework. In this case, the Consumer may need to interact directly with the Producer Knode.

Purpose Statement

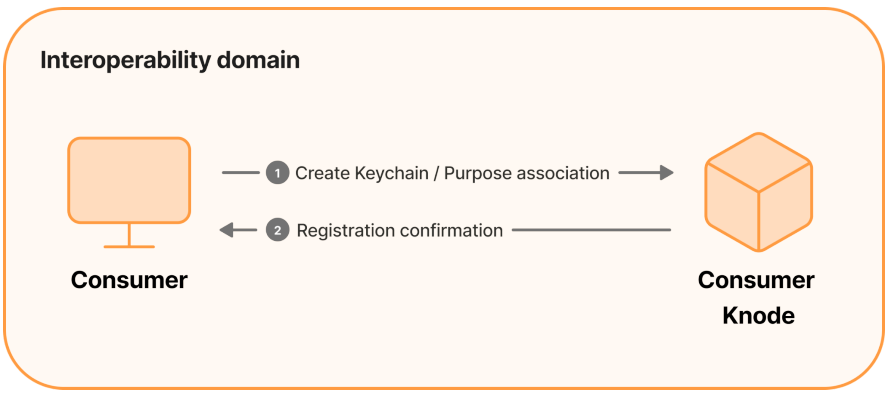
When the Agreement Request is approved, the Consumer declares the conditions for the lawfulness of processing (pursuant to Article 6 of the *GDPR*), which allow it to acquire personal data through the Cross-Border E-Service. The Consumer interacts directly with the Consumer Knode, which forwards the statement to the Producer Knode.



The Producer Knode can request additional information from the Consumer to implement the national regulatory framework regarding the protection of personal data of natural persons. In this case, the Consumer may need to interact directly with the Producer Knode.

Keychain association

The Consumer associates one or more *Keychains* registered on the Consumer Knode with the Purpose Statements made. The Consumer deposits in the Keychains the cryptographic material used by its IT systems (hereinafter, clients) to access the Cross-Border E-Service.

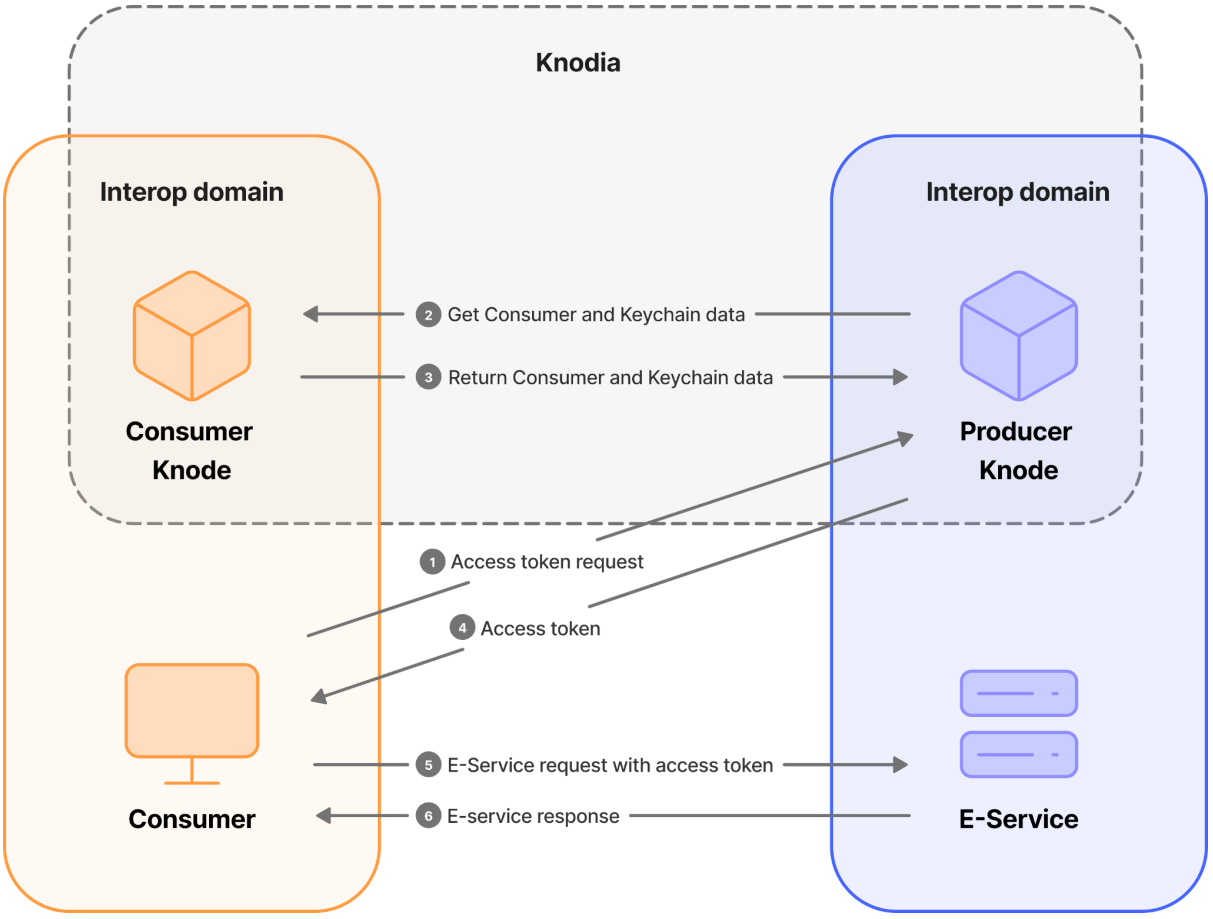


Access to a Cross-Border E-Service

The information that the Producer Knode has received and Electronically Archived in the steps described so far constitutes the technical-administrative prerequisites enabling the Producer Knode to issue access tokens to the Consumer's clients to access the Producer's E-Service.

To access a Cross-Border E-Service, the following steps must occur:

1. The Consumer's client constructs the request to send to the Producer Knode to obtain an access token related to one of the Purpose Statements. It electronically seals the request, using the private cryptographic material corresponding to the public material deposited in the Keychain, and sends it to the Producer Knode.
2. The Producer Knode compares the request content with the information it has Electronically Archived. It authenticates the client, interacting with the Consumer Knode to verify the seal using the public cryptographic material deposited in the Keychain. If verification succeeds, it issues an access token to the Consumer's client.
3. The Consumer's client sends a request to the Producer's E-Service using the Producer Knode's access token.
4. The Producer's E-Service verifies the validity and integrity of the received access token. If verification succeeds, it prepares and sends the response to the Consumer's client.



Additional functionality provided by Knodes

In addition to enabling the core E-Service consumption flow illustrated above, Knodes provide additional functionality. This includes the following.

- Knodes must allow Producers to respond to Consumer requests asynchronously, rather than synchronously (for example, for E-Services that require longer processing times).
- In addition to the standard usage model (whereby a Consumer calls the E-Services made available by Producers), Knodes can provide a signal distribution mechanism. This allows the Consumer to know, for an E-Service that they have been enabled to use, when changes occur to the data provided by that E-Service for the entities of interest to the Consumer.
- A Cross-Border E-Service Template standardizes the process of creating Cross-Border E-Services for recurring use cases. If many Producers need to provide the same E-Service, one Producer can create a Template and make it available in its Knode so that other Producers who need to provide an E-Service with similar characteristics can instantiate it.
- A Knode can allow Producers to register one or more *Producer Keychains* to associate with their Cross-Border E-Services. Producer Keychains (like the Keychains for Consumers described above) are repositories of cryptographic material. They allow Producers to sign the responses returned by their Cross-Border E-Services to guarantee non-repudiation.

Expected benefits and features

The proposed cross-border federation realized by *Knodia* ensures that:

- The attribution of responsibilities to the subjects involved in the functioning of the ecosystem is certain.
- APIs made available by Producers are published on the Cross-Border E-Service Catalogue of the Knode on which the Producer is identified.
- Access to APIs occurs securely upon completion of actions and declarations made by Consumers and upon (implicit or explicit) acceptance by Producers.
- Interaction occurs directly between Producers and Consumers, in synchronous or asynchronous modes, without intermediation components that can be potential single points of failure.
- A technical architecture is defined for the components necessary to implement the ecosystem.
- Open standards define the communication protocols used by the ecosystem components.
- Templates for APIs and declarations of lawfulness of personal data processing are available to simplify usage by Confederate Organizations.
- Both human-oriented and machine-to-machine interfaces are available to let Confederate Organizations use the functionality provided by Knodes.
- The necessary tools are available for Confederate Organizations to deposit on the Knodes the cryptographic material required to secure interactions, in public key and X.509 certificate formats.
- Producers can request Consumers of their APIs proof of possession of the cryptographic material deposited by the latter on the Knodes.
- The Knodes provide functionality useful to notify interested Consumers of changes to data held by the Producers.

The following table summarizes the key features of Knodia as proposed.

	Characteristic	**Knodia**
Technological aspects	**Interaction technologies**	• HTTP APIs
	Authentication standards	• OAuth2 • JWT • JWK
	Development model	• open source
Operative aspects	**Initial setup**	• one-off for interested parties
	Agreement management	• *GDPR*-compliant process based on agreement requests and purpose statements
	Maintenance	• Knodes only
	Infrastructure costs	• Knodes only

Knodia

	Characteristic	Knodia
	Monitoring	● centralized in Knodes
Functionality	**E-Service versioning**	● centralized tools
	E-Service discovery	● using Knode E-Service Catalogues
	Confederate Organization categorization	● centralized attribute management
	E-Service co-design	● possible using E-Service Templates
	Data variation distribution	● standardized and centralized
Governance and compliance	**Regulatory compliance**	● adaptable to national regulatory frameworks in individual Knodes
	Application of the once-only principle	● natively supported
	GDPR compliance	● standardized and centrally managed purpose statement ● pre-filled purpose statement templates
	Traceability of interactions	● centralized in individual Knodes
	Exchange audit	● simplified by centralizing evidence in individual Knodes

STAKEHOLDERS

Dipartimento per la trasformazione digitale

PagoPA S.p.A.