Knodia

Cross-Border Federated Interoperability

WHITEPAPER

Get in touch — info@knodia.org

---

v1.0 15 January 2026

Table of contents

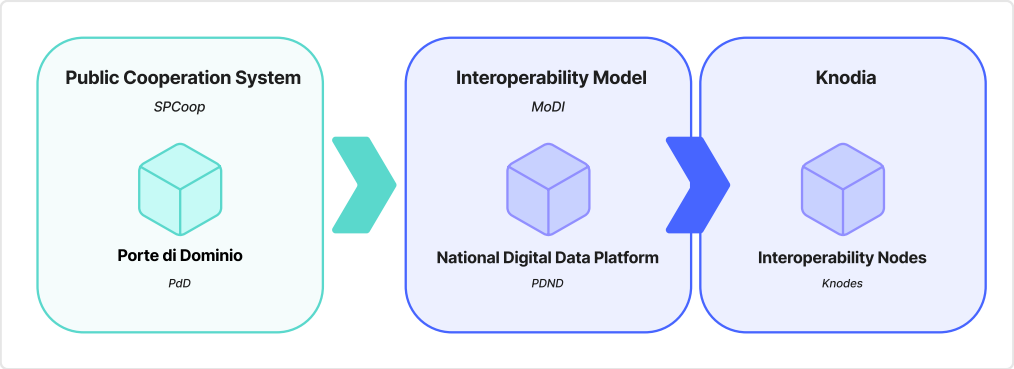
Chapter 1

Abstract

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.

Knodia, a *cross-border authentication and authorization framework*, is intended as a technical and administrative solution to enable digital interaction between organizations in different Member States, as well as between these organizations and the agencies of the *European Commission* and, in general, the *European Union*. The solution implements the API-first approach and is intended to ease the implementation of the once-only principle.

The *Knodia* proposal originates from the positive experience of the *Piattaforma Digitale Nazionale Dati* in Italy (*PDND*). The latter is the infrastructure for authentication and authorization of organizations – both public and private – within the *Interoperability Model* (*ModI*) for 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.

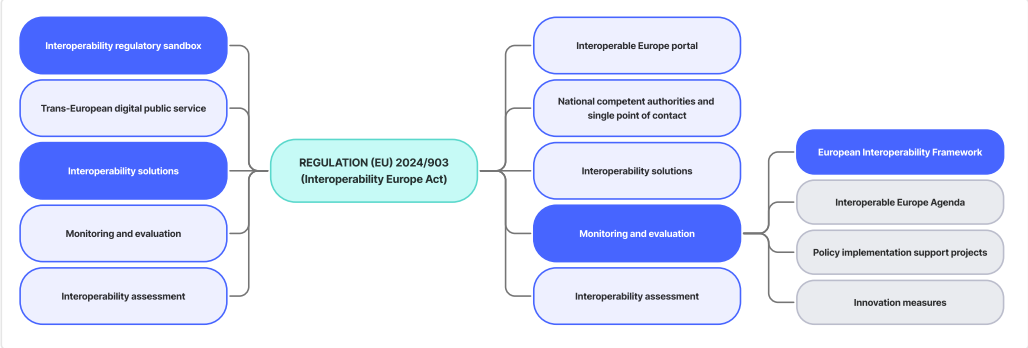
This document is organized into four distinct chapters. Specifically:

- **2 "Regulatory context"** considers this proposal in light of Regulation (EU) 2024/903.
- **3 "Objective of the proposal"** presents the objectives that this proposal intends to fulfil.
- **4 "Knodia as an evolution of the Italian interoperability experience"** summarizes the Italian experience on interoperability from which this proposal originates.
- **5 "Knodia: cross-border federated interoperability"** describes the elements that compose *Knodia* and how its members can implement it.

Chapter 2

Regulatory context

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[1] (in brief, the *Interoperable Europe Act*), entered into force on 18 July 2024. It aims to foster and simplify interactions between the European Union and Member States, and equally among Member States themselves, to facilitate the sharing of data, information, and knowledge through digital processes (*cross-border interoperability*).



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 within its scope.

The European Commission adopts the *EIF* to define cross-border and cross-sector *interoperability solutions* based on open standards and specifications.

The *Interoperable Europe Board* (defined in Article 15 of the *Interoperable Europe Act*) is tasked with drafting and presenting the *EIF* to the European Commission for adoption (pursuant to section 6 of the *Interoperable Europe Act*).

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**

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R0903

and Social Committee and the Committee of the Regions (COM/2017/0134 final) regarding the European Interoperability Framework – Implementation Strategy[2].

The *Interoperable Europe Act* allows for the creation of *interoperability regulatory sandboxes*, also for "fostering innovation and facilitating the development and roll-out of innovative digital *interoperability solutions* for public services" (Article 11 of the *Interoperable Europe Act*).

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A134%3AFIN

Chapter 3

Objective of the proposal

The *EIF* provides guidance to European public administrations through recommendations on how to improve the governance of their interoperability activities to:

- Foster and simplify interactions between the European Union and Member States, and among Member States themselves, to promote the sharing of data, information, and knowledge through digital processes.
- Avoid the creation of fragmented ICT islands whose interoperability is difficult to guarantee.

The objectives of the *EIF* are met through the realization of 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*.

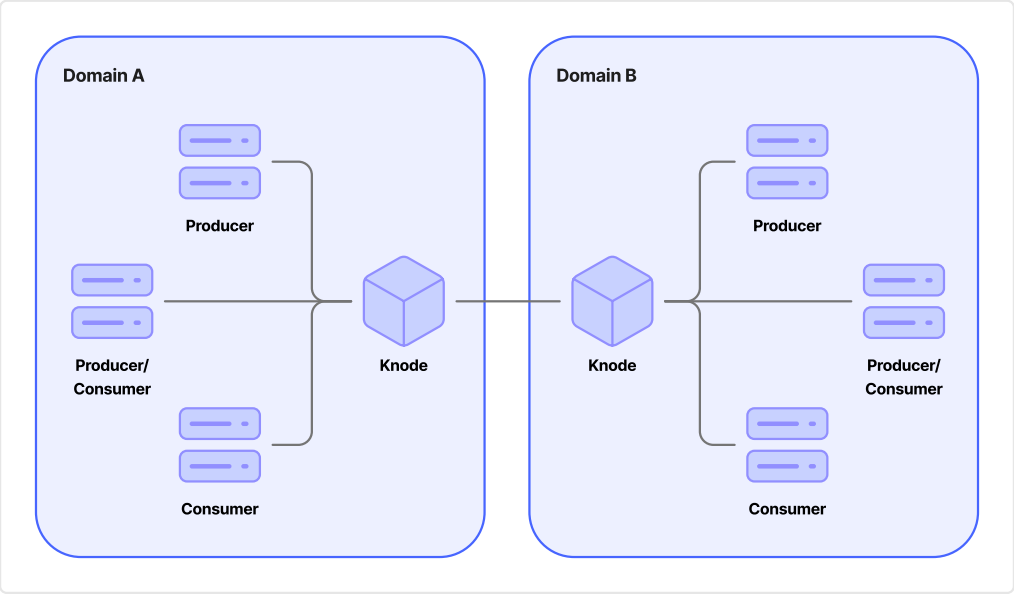
In this scenario, regardless of the specific application domain that the interaction between interested parties involves, there is the need to authenticate and authorize access to APIs and ensure their usage in compliance with the regulatory framework regarding the protection of personal data of natural 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**[1] (*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 present proposal, within the framework of the *Interoperable Europe Act* and specifically the instrument of *interoperability regulatory sandboxes*, proposes to establish a technical-administrative framework, hereinafter named *Knodia*, that, at a cross-border level, manages authentication and authorization for access to APIs by the organizations involved (constituting a cross-border federation).

The definition of *Knodia*, which capitalizes on the Italian experience of the *Piattaforma Digitale Nazionale Dati* (*PDND*), pursues the following objectives:

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

- 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 *Confederate Organizations* that can request access to their APIs based on the *attributes* the latter possess.
- 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.



Knodia as a whole constitutes the digital ecosystem involving:

- *Producer Confederate Organizations*: the organizations that make APIs available for access to data for which they are the authoritative source.
- *Consumer Confederate Organizations*: the organizations that, to perform their activities pursuant to current legislation, access the APIs made available by the Producers.
- *Interoperability Nodes* (hereinafter, *Knodes*): the entities that manage a domain by identifying a set of *Confederate Organizations* and providing services to them to operate within the ecosystem.

In the digital ecosystem constituted by *Knodia*:

- A *Confederate Organization* can be simultaneously both a *Producer* and a *Consumer*.
- *Producer-Consumer* interactions always occur between two *Confederate Organizations* belonging to distinct domains.

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 or 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.

This proposal will be supplemented by the preparation of a prototype of the application components necessary to realize *Knodia*, which will be made available to subjects interested in verifying its functionality.

Chapter 4

Knodia as an evolution of the Italian interoperability experience

Knodia, the subject of this proposal, benefits from the experience of Italian public entities in sharing data and services among themselves and with private entities (businesses and citizens) as a prerequisite for implementing the once-only principle.

The Italian experience in this matter has seen two main stages:

- **Application cooperation (*cooperazione applicativa*):** Adopted from 2008 to 2021, this outlined the technical implementation framework of the *public cooperation system* (*sistema pubblico di cooperazione*), also known as *SPCoop*, as the conceptual and architectural model of application cooperation between Italian public entities.
- **Interoperability (*interoperabilità*):** Adopted from 2022 to the present, this identified the *interoperability model* (*modello di interoperabilità*, briefly *ModI*), characterized by the *PDND* infrastructure, as an evolution of *SPCoop*. It aimed at increasing cooperation between public entities and extending interactions to private entities by means of technological solutions that ensure interaction and information exchange without constraints on implementations.

The following sections summarize the characteristics of *SPCoop* and *ModI*, the elements considered by the Italian public administration that motivated the paradigm shift, and the benefits derived from the functionalities made available by the *PDND* for interested parties.

4.1 The Italian public cooperation system

The *SPCoop* constituted the conceptual and architectural model of application cooperation between Italian public entities. It aspired to:

1. Define the method of delivering application services to realize interactions between cooperating entities.
2. Ensure parity among all cooperating entities and the separation of respective responsibilities.
3. Guarantee the independence of cooperating entities in relation to their organizational structures and the management of their IT systems.
4. Delegate to individual cooperating entities the responsibility for authorizing access to data and/or services they provide.

The adoption of the *SPCoop* by Italian public administrations derived from the provisions of the **Decreto del Presidente del Consiglio dei Ministri del 1 aprile 2008 - Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82**[1]. It was fully delineated at the technical-implementation level by guidelines that mandated the use of well-established standards at the time of their adoption.

The *SPCoop* was based on the following principles:

- **Cooperation between administrations:** Public entities cooperated by providing and using application services. Such services were offered by each public entity through a single component of its IT system called the *Porta di Dominio*.
- **Scope of responsibility:** Each cooperating public entity maintained responsibility for the services it provided and the data supplied through such services.
- **Service agreements:** An application service operated on the basis of agreements stipulated between at least two entities (producer and consumer), based on consultation between them, and subsequently formalized by them in *Service Agreements* (*Accordi di Servizio*), a semi-automatic representation based on XML language.
- **Cooperation technologies:** Application services were provided and consumed through remote invocation technologies and standards. This followed international standards (W3C[2] and OASIS[3]) at the time of *SPCoop* adoption, specifically:
  - Simple Object Access Protocol (SOAP) as the application protocol for remote service invocation.
  - Web Service Description Language (WSDL) as the language for interface description.
  - Universal Description, Discovery, and Invocation (UDDI) as the architecture and interface of the registry of provided services, with access predominantly based on unique identifiers.

  These were completed by defining national standards, such as the extension to

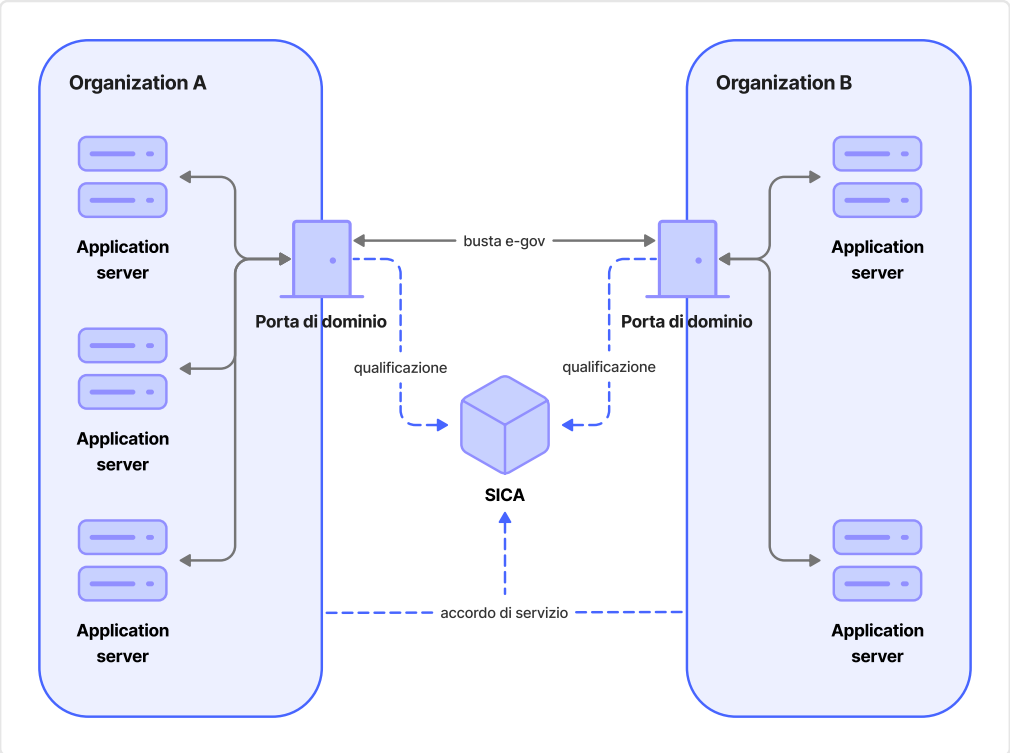
[1] https://www.gazzettaufficiale.it/eli/id/2008/06/21/08A04425/sg
[2] https://www.w3.org/
[3] https://www.oasis-open.org/

SOAP called *busta e-gov*, to meet the objectives of the *SPCoop*.

In summary, the *SPCoop* was based on the Service-Oriented Computing paradigm and organized as a Service-Oriented Architecture, by adopting international technologies and standards, extended and integrated to make this architecture suitable for the Italian e-Government context.

To mediate and support cooperation between administrations, the *SPCoop* provided for an infrastructural component, called *Servizi di Interoperabilità, Cooperazione ed Accesso* (*SICA*). This provided infrastructure and technological services (registry services, security services, etc.). In particular, the Certification Authority required to manage a Public Key Infrastructure (PKI) – the base mechanism for all cryptographic aspects supporting the security of *SPCoop* – was instantiated within the *SICA* security services.

The following figure shows the high-level architecture of the *SPCoop*. It emphasizes that *Service Agreements* were stipulated autonomously by the interested parties, without the tools made available in the *SPCoop* for this. Their formalization and upload, also the responsibility of the interested parties, were needed to register with the *SICA*.



4.2 The Italian interoperability model

The *ModI* considers the digital services (hereinafter *e-services*) created by public entities to ensure access to their data and/or services through the interaction of their

IT systems with those of other entities that, in compliance with current legislation, need to interact with them to perform their activities.

The *ModI* critically evolved the *SPCoop* based on experience gained from its application to overcome the factors that limited its diffusion.

The adoption of the *ModI* by Italian public administrations is provided for by the **Decreto Legislativo del 7 marzo 2005, n. 82** and, specifically, by:

- Article 73, paragraph 3-ter, letter b), regarding the adoption of guidelines and rules for cooperation and interoperability.
- Article 50-ter, paragraph 2, regarding the *Piattaforma Digitale Nazionale Dati* (briefly *PDND*) as the technological infrastructure that enables the interoperability of IT systems and databases between public entities and between these and private entities.

Operationally, the *ModI* is regulated by guidelines adopted by the *Agenzia per l'Italia Digitale*, in agreement with the *Dipartimento per la trasformazione digitale*, and constantly updated, also by incorporating requests from interested parties.

The *ModI* is based on the following principles:

- **Interactions:** Interactions assume that the involved entities, public and private, can perform the function of *Producer* of *e-services*, when they make digital services available to other entities, and the function of *Consumer* of *e-services*, when they use the *e-services* made available by another entity.
- **Application programming interface:** The *e-services* made available by *Producers* are implemented by application programming interfaces (APIs) using either of these technologies and standards for remote invocation:
  - SOAP over HTTP and the so-called WS-* stack.
  - REST APIs, classifiable at Level 1 of the Richardson Maturity Model, hereinafter HTTP APIs.
- **Interoperability patterns and profiles:** These are progressively identified with the involvement of interested parties. These define solutions to secure data exchange needs, which *Producers* use to implement their *e-services*.
- **Division of responsibilities:** *Producers* are responsible for the *e-services* they provide, while *Consumers* are responsible for managing the data they receive.
- **Cooperation technologies:** *E-services* are provided and consumed through technologies and standards for remote invocation, standardized (*de iure* and *de facto*) at the international level (W3C[4], Internet Engineering Task Force[5], and Linux Foundation[6]). Specifically:
  - *Regarding SOAP over HTTP e-service implementations:*
    - Simple Object Access Protocol (SOAP), as the application protocol for remote service invocation.
    - Web Service Description Language (WSDL), as the language for interface

[4] https://www.w3.org/
[5] https://www.ietf.org/
[6] https://www.linuxfoundation.org/

description.
- *Regarding HTTP API e-service implementations:*
  - RFC3230, RFC3744, RFC5246, RFC5789, RFC7231, RFC7233, RFC7389, RFC7396, RFC7515, RFC7519, RFC8725, RFC9110, for the implementation of application interfaces (API).
  - OpenAPI Specification, as the language for interface description.
- *Regarding services offered by the PDND:*
  - RFC6749, RFC6750, RFC7235, RFC7515, RFC7523, RFC9449, for the issuance of authorization tokens.
  - RFC7517, RFC7696, for public key management.
  - RFC3230, RFC3744, RFC5246, RFC5789, RFC7231, RFC7233, RFC7389, RFC7396, RFC7515, RFC7519, RFC8725, RFC9110, for the implementation of application interfaces (API).
  - OpenAPI Specification, as the language for interface description.

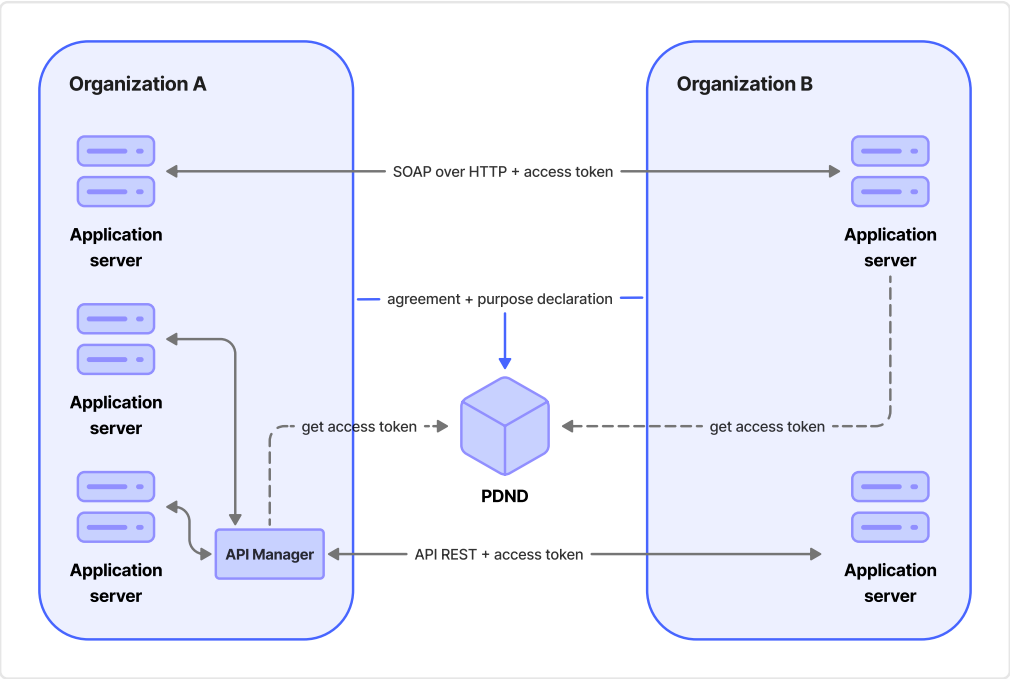
The *ModI* preserves the adoption of the Service-Oriented Computing paradigm and the organization as a Service-Oriented Architecture of the *SPCoop*. It includes the *PDND* in its reference architecture as an infrastructural component that provides services to *Producers* and *Consumers* (generally referred to as *Organizations*) to enable their interaction. In particular:

- It authenticates *Organizations* based on their identification at the time of onboarding to the *PDND* and throughout their membership. This is achieved by integration with authoritative sources, such as, by way of example, the *Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi* (*IPA* – index of digital domiciles of public administrations and private providers of public services) and the *Indice nazionale delle imprese e dei professionisti* (*INI-PEC* – national index of enterprises and professionals).
- It assigns peculiar characteristics to *Organizations* and maintains them through the mechanism of certified attributes, based on feedback from authoritative sources regarding supervisory or control authorities integrated with the *PDND*.
- It provides an *API Catalogue* that lets *Consumers* verify the availability of *e-services* published by *Producers*, regardless of whether they can be accessed.
- It provides tools to *Producers* to manage the lifecycle (creation, publication, update, suspension, restoration, deprecation, archiving, and versioning) of their *e-services* published on the *API Catalogue*, including reporting regarding their usage by *Consumers*.
- It allows *Producers*, when publishing their *e-services*, to specify whether *Consumers* must use bearer tokens or tokens that demonstrate proof of possession of cryptographic material (*DPoP*-bound tokens).
- It allows *Producers* to publish *e-services* that permit *Consumers* either to access data held by the *Producer* or to forward data in their possession to the *Producer*.
- It manages agreement requests that allow potential *Consumers* (who possess the certified attributes required by *Producers* at the time of publishing their *e-services*) to signal the intention to use a specific *e-service*. It leaves it to the *Producer* to either be informed only of the request or explicitly approve it.

- It manages statements of purpose – a prerequisite for using *e-services* – for approved agreement requests, so that *Organizations* that receive data can record the motivation and regulatory prerequisites justifying the use of the data they obtained via *e-services* (e.g., the lawfulness of processing under the *GDPR*).
- It records API clients used by *Consumers* to access *e-services* relative to the declared purposes and the cryptographic material associated with said clients, primarily needed for preliminary authentication to the *PDND* for the issuance of authorization tokens for access to *e-services*.
- It issues authorization tokens (bearer tokens or *DPoP*-bound tokens) for *Consumers* to access *e-services*. To do so, it verifies the completion of the purpose statement by the *Organization* receiving new data and the status of the associated agreement request.
- It supports an asynchronous message exchange model for interactions between *Producers* and *Consumers* for an *e-service*, enabling the inclusion of the necessary elements in the authorization tokens.
- It makes *e-service* templates available as a co-design tool to facilitate coordination across application domains where several *Organizations* provide analogous *e-services*. It also makes pre-compiled models of purpose statements available to simplify the statement incumbent on *Organizations*.
- It provides tools that allow *Producers* to communicate evidence of changes to data provided by their *e-services* to *Consumers* who need to manage these changes, in a manner consistent with the regulatory framework.

In short, the *PDND* serves as an *Authentication and Authorization Server*. It applies the Attribute-Based Access Control model regarding the agreement requests initiated by *Consumers* and integrated with purpose statements by *Organizations* to enable access to *e-services*. It ensures the issuance of authorization tokens to permit interactions between the IT systems of *Producers* and *Consumers*. Furthermore, the *PDND* provides *Organizations* with the services necessary for their full participation in the *ModI*, in compliance with current legislation, with particular attention to the protection of personal data, within an administrative and technological security framework for *Organizations*.

The following diagram illustrates the high-level architecture of the *ModI*.



Within the *ModI*, the *PDND*, in addition to performing the function of an *Authentication and Authorization Server*, supports and standardizes *Organizations'* processes, particularly for enabling the use of *e-services*.

4.3 Evolution from the public cooperation system to the interoperability model

This section explains the rationale for Italy's transition from the *SPCoop* to the *ModI*.

The *SPCoop* launched the Italian experience in data sharing and service integration between Italian public administrations via digital tools. However, experience with it highlighted that:

- The *Porta di Dominio* component of the technological architecture (which used the custom SOAP extension named *busta e-gov*) required public administrations to adopt this component, risking technological lock-in.
- The *Porta di Dominio* component was imposed on public administrations, reducing their freedom to make internal choices within each organization. This circumstance was most relevant in complex public administrations that applied aggressive segmentation policies to their server farms, or in public administrations that began adopting cloud computing.
- Delegating to individual cooperating entities the responsibility for authorizing access to their provided data and/or services (through agreements between parties) delayed public administrations' participation due to frequent duplication of administrative proceedings.

- Defining a unique security framework – regardless of the nature of the data subject to interaction – overburdens public administrations participating in interactions, even in cases where the data to be exchanged could have allowed a less onerous approach.

Italy re-evaluated the *SPCoop* after the consolidation of the European regulatory framework regarding interoperability, the opening of public data, and the protection of personal data of natural persons, primarily through:

- **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**[7].
- **Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information**[8].
- **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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**[9].

The choice was ultimately reinforced by the **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**[10].

The technological evolution since the launch of the *SPCoop* has highlighted the opportunity to re-evaluate the technologies used to ensure data sharing and service integration among Italian administrations. In particular, the increased use of HTTP APIs, even in complex contexts, and the availability of tools for implementing and managing them. It is also worth noting that the evidence of increased use of HTTP APIs is supported by the interest shown by international organizations and initiatives, such as:

- W3C[11].
- Internet Engineering Task Force[12].
- Linux Foundation[13].

Over the years, these have increased *de iure* and *de facto* standardization actions. This led to an increase in the market offer of technological solutions and an increased availability of the professionals necessary for their maintenance. This circumstance can create the prerequisites for reducing costs in the management of public administration technological infrastructures.

Considering the above, Italy defined the *ModI* based, primarily, on the following

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A134%3AFIN
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R0903
[11] https://www.w3.org/
[12] https://www.ietf.org/
[13] https://www.linuxfoundation.org/

choices:

- Increasing the degree of freedom of entities interested in interactions. Specifically, this concerns organizational and technological choices: relaxing the constraint of the Porte di Dominio and, to guarantee interoperability, selecting international standards for specific interaction needs (interoperability patterns and profiles).
- Expanding the services offered by the infrastructural component, specifically the *PDND*, and in particular delegating to it:
  - Certain identification of interested parties (onboarding) and management of their authorization titles (attribute management).
  - Providing entities that must/want to interact with a normalized process (agreement requests and purpose statements), compliant with provisions regarding the protection of personal data of natural persons.
  - Distributing public cryptographic material used by entities involved in transactions.
  - Issue authorization for API access (issuance of access tokens) based on the status of interested parties and the evidence recorded from their agreement requests and purpose statements.
  - Providing tools to facilitate interested parties, specifically to:
    - Support API design (*e-service* templates).
    - Simplify application of the *GDPR* (pre-compiled purpose statement templates).
    - Create APIs for data reception (*reverse production* / *Receive-Data* mode).
    - Manage interactions with a high processing burden for response preparation (asynchronous communication).
    - Distribute data changes to interested parties entitled to them (*Signal Hub*).

The following table provides a synoptic comparison between the *SPCoop* and the *ModI*.

Criterion	*SPCoop* (application cooperation)	*ModI* (interoperability) based on the *PDND*
Period of adoption	• 2008–2021	• 2022–present
Interested subjects	• public administrations	• public administrations • providers of public services • enterprises

Technologies and standards	• SOAP
	• WSDL
	• UDDI
	• *busta e-gov*
		• HTTP APIs
		  • RFC3230, RFC3744, RFC5246, RFC5789, RFC7231, RFC7233, RFC7389, RFC7396, RFC7515, RFC7519, RFC8725, RFC9110
		  • OpenAPI Specification
		• SOAP
		  • SOAP
		  • WSDL

Onboarding	• Qualification of the *Porta di Dominio*	• Onboarding of the organization to the *PDND*

Enabling interactions	• Autonomous stipulation of Service Agreements between interested parties	• Centralized normalized process managed by the *PDND*:
		  • agreement request
		  • purpose statement
		  • API client registration

Key components	• *Porta di Dominio* (for service delivery) • *SICA* (interoperability, cooperation and access services)	• *PDND* (technological infrastructure and centralized authentication and authorization server; centralized API Catalogue)

Infrastructure components and services	• *SICA*
	  • Registry Services
	  • Subject Index Services
	  • Security Services
		• *PDND*
		  • Onboarding of organizations and attribute assignment
		  • API Catalogue of provided e-services
		  • E-service lifecycle management
		  • Agreement request for an e-service
		  • Purpose statements
		  • API client management
		  • Authorization token issuance
		  • Reverse production
		  • Asynchronous communications
		  • E-service templates
		  • Pre-compiled purpose statement templates
		  • *Signal Hub*

Adoption numbers	• Total qualified *Porte di Dominio*: 288 of which 91 active as of 25-06-2023 (source: "Porte di dominio" dataset of the *Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi* (*IPA*), https://indicepa.gov.it/ipa-dati/dataset/porte-di-dominio)	• 8,787 onboarded entities (public and private) • 13,122 published e-services • 21,336 connections between entities • 834,745,611 exchange sessions N.B. the indicated data reflects status as of 23-10-2025 (source: "I numeri della PDND", https://www.interop.pagopa.it/numeri, in open format at URL https://www.dati.gov.it/view-dataset?tags=pdnd&organization=pcm-dipartimento-trasformazione-digitale&page=0)

The principal value of the Italian decision to transition from the *SPCoop* to the *ModI*, to date, is supported by the significant increase in adoption: 8,621 public entities have onboarded to the *PDND* compared to 288 equipped with qualified *Porte di Dominio* in the *SPCoop*.

Furthermore:

- The number of connections between public and private entities – 21,336 – is evidently a result of the simplification enabled by *PDND*'s services for *Organizations* to ease these actions (particularly agreement requests and purpose statements).
- The number of exchange sessions between *Producers* and *Consumers* exceeds 834,745,611, where multiple interactions can occur within a single session.

For a correct interpretation of the reported numerical evidence, it is worth noting that onboarding to the *PDND* began in October 2022 for public entities and in June 2025 for private entities.

The objective evidence of the positive effects of adopting the *ModI* through the *PDND* in the Italian context forms the basis of this proposal.

4.4 Comparing *Porte di Dominio* and *PDND*

What follows is a comparative analysis of the *ModI* and the *SPCoop*. This focuses on the technological components necessary for subjects interested in applying either model, respectively the *PDND* and the *Porte di Dominio* (though these play different roles in the two architectures, as described previously).

The following criteria are examined considering the burdens and possibilities for subjects interested in participating in interactions in the two models. Burdens and possibilities are evaluated as either:

- ✅ – positive for subjects interested in participating in interactions.
- ⚠️ – burdensome for subjects interested in participating in interactions.
- ❌ – functionality not available for subjects interested in participating in interactions.

The comparative analysis highlights the advantages obtained in transitioning from *Porte di Dominio* to the *PDND*. In brief, these are:

- The definition of a normalized process, shared among all interested subjects, to enable access to *e-services* and allow interaction between them.
- The adoption of technologies that are in wider use and have lower complexity, which can potentially reduce costs.
- The centralized sharing, via the *PDND*'s API Catalogue, of the offer of digital services, to facilitate meeting demand with supply.
- The security framework based on the *PDND* which ensures: the authentication and authorization of access to *e-services*; the protection, integrity, and confidentiality of the data exchanged; and the complete traceability of requests and their outcome.

4.4.1 Technological aspects

Criterion	*Porte di Dominio*	*PDND*
Interaction technologies	⚠ *busta e-gov*	✅ HTTP APIs ⚠ SOAP over HTTP
Authentication standards	⚠ WS-Security ✅ X.509 certificate	✅ OAuth2 ✅ JWT ✅ JWK
Development model	⚠ on-premise	✅ open source
Technical complexity	⚠ medium-high	✅ low-medium

4.4.2 Operative aspects

Criterion	*Porte di Dominio*	*PDND*
Initial setup	⚠ installation and qualification for each *Porta di Dominio* instance of the interested party	✅ one-off for interested parties
Agreement management	❌ direct relation between interested parties	✅ unique, *GDPR*-compliant process based on agreement requests and purpose statements
Maintenance	⚠ each *Porta di Dominio* instance of the interested party	✅ single point of interest
Infrastructure costs	⚠ cost center for each *Porta di Dominio* instance of the interested party	✅ single cost center
Monitoring	⚠ distributed for each *Porta di Dominio* instance of the subject	✅ centralized

4.4.3 Functionality

Criterion	*Porte di Dominio*	*PDND*
E-service versioning	⚠ distributed for each *Porta di Dominio* instance of the subject	✅ centralized tools
E-service discovery	❌ direct relation between interested parties	✅ centralized via API Catalogue
Subject categorization	❌ realized by interested parties towards each other	✅ centralized via attribute management
E-service co-design	❌ direct relation between interested parties	✅ API templates
Data variation distribution	⚠ implemented by interested parties for individual e-services	✅ standardized and centralized via the *Signal Hub*

4.4.4 Governance and compliance

Criterion	*Porte di Dominio*	*PDND*
Regulatory compliance	⚠ conforms to outdated regulatory framework	✅ conforms to current Italian regulatory framework
Once-only principle application	❌ direct relation between interested parties	✅ favoured in a native manner
***GDPR* application**	❌ realized by interested parties	✅ uniform purpose statement managed centrally ✅ pre-compiled purpose statement templates
Interaction traceability	⚠ distributed for each *Porta di Dominio* instance of the subject	✅ complete and centralized
Exchange audit	⚠ distributed for each *Porta di Dominio* instance of the subject	✅ simplified by centralization of evidence
Future roadmap	❌ phasing out	✅ investments in progress

4.4.5 Ecosystem and support

Criterion	*Porte di Dominio*	*PDND*
Community	❌ realized by interested parties	✅ growing, current support from the Italian Regulator
Documentation	⚠️ not maintained	✅ modern and updated
Availability of dev tools	❌ not available for *busta e-gov*	✅ high for HTTP APIs ⚠️ limited for SOAP over HTTP
Availability of tech skills	⚠️ very limited for *busta e-gov*	✅ high for HTTP APIs ⚠️ limited for SOAP over HTTP

Chapter 5

Knodia: cross-border federated interoperability

This chapter outlines the features that the actors involved in *Knodia*, primarily the *Knodes*, must provide to enable interoperability between multiple independent *Knodia Domains*.

Knodia extends the Italian interoperability model based on the *PDND*, introduced in the previous chapter and adopted in Italy to enable interaction between the IT systems of public administrations and between these systems and those of recognized private subjects.

Knodia is meant to support a case like that of the European Union. Each *Knodia Domain* – corresponding to a Member State or, more generally, to a set of organizations identified with certainty (such as the agencies of the European Commission) – maintains its autonomy regarding interoperability within its perimeter of competence. The objective here is to allow digital interaction between the IT systems of the organizations of these *Knodia Domains* through shared mechanisms based on mutual inter-domain trust. These interactions are hereinafter referred to as *cross-border interactions*.

Knodia is designed in compliance with *EIF* Recommendation 26. Concerning interoperability agreements between organizations in the provision of a European public service, the Recommendation requires to "establish interoperability agreements in all layers, complemented by operational agreements". Specifically, within *Knodia*, the cited interoperability agreements are digitally materialized through the authentication of the involved organizations and the execution of the actions required to verify the regulatory prerequisites for sharing data and services between them. The related operational agreements are implemented by defining and sharing mechanisms implemented within the IT systems of the organizations interested in *cross-border interactions*.

Knodia considers the interoperability levels described by the *EIF* itself, specifically:

- *Legal interoperability:* ensures compliance with the European regulatory framework on interoperability and on the protection of personal data of natural persons,

preserving the possibility of integrations by Member States.
- *Organizational interoperability:* specifies the relationships between the organizations involved and the processes they follow to enable *cross-border interactions* between them.
- *Semantic interoperability:* identifies the shared semantic objects (controlled vocabularies, ontologies, and data schemas) necessary to enable *cross-border interactions*.
- *Technical interoperability:* defines a shared federated protocol that interested organizations implement to enable *cross-border interactions* between their IT systems.

5.1 A federation of Knodes

Within *Knodia*, *cross-border interactions* for sharing data and/or integrating services are enabled through *Cross-Border E-Services*.

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

Knodia provides for the existence of the following actors:

- The *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:
  - *Producer*, when they provide *Cross-Border E-Services* to other *Confederate Organizations*.
  - *Consumers*, when they consume the *Cross-Border 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 *Knodia Consortium*) is necessary to establish the governance of *Knodia*. 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 perform *cross-border interactions* with each other and 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*.

5.1.1 Cross-Border E-Service consumption flow

To ease the reading of the subsequent sections, 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*.

5.1.1.1 Cross-Border E-Service publication

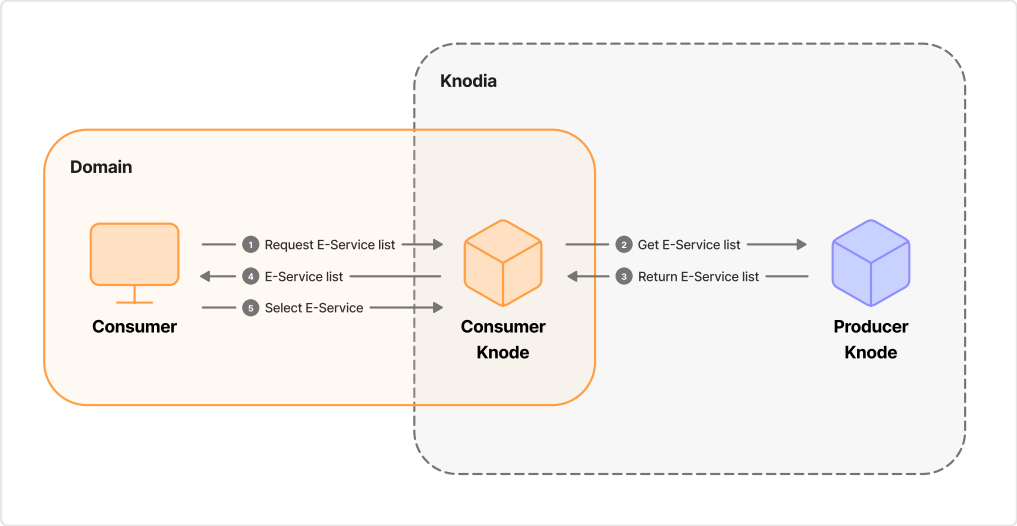
The *Producer* registers the *Cross-Border E-Service* on the *Producer Knode* to enable cross-border usage. This includes defining the *consumption requirements*, which are the characteristics (*Attributes*) that potential *Consumers* must satisfy to access the *E-Service*.

See § 5.4.1 “Cross-Border E-Service publication” for details.

5.1.1.2 Cross-Border E-Service discovery

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

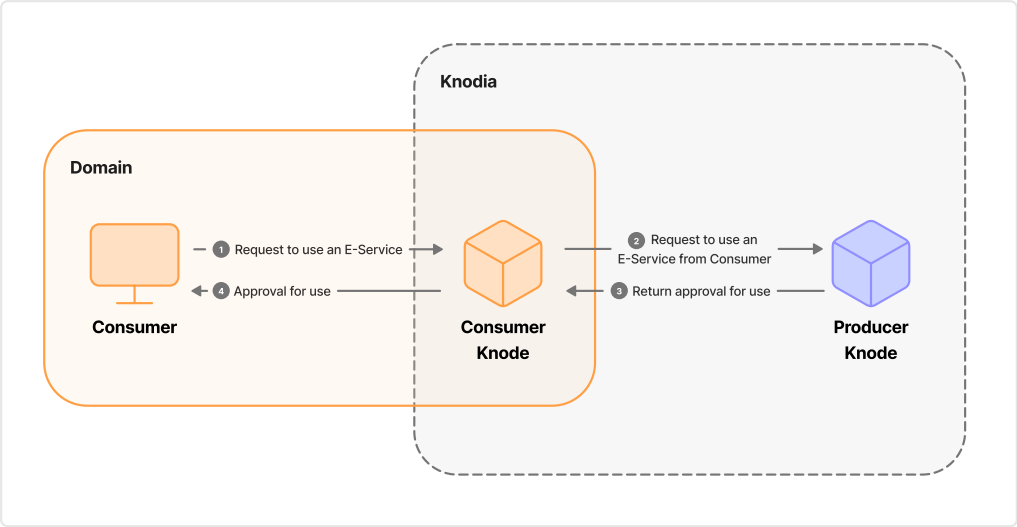
See § 5.4.2 “Cross-Border E-Service discovery” for details.



5.1.1.3 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*.

See § 5.5.1 “Agreement Request” for details.

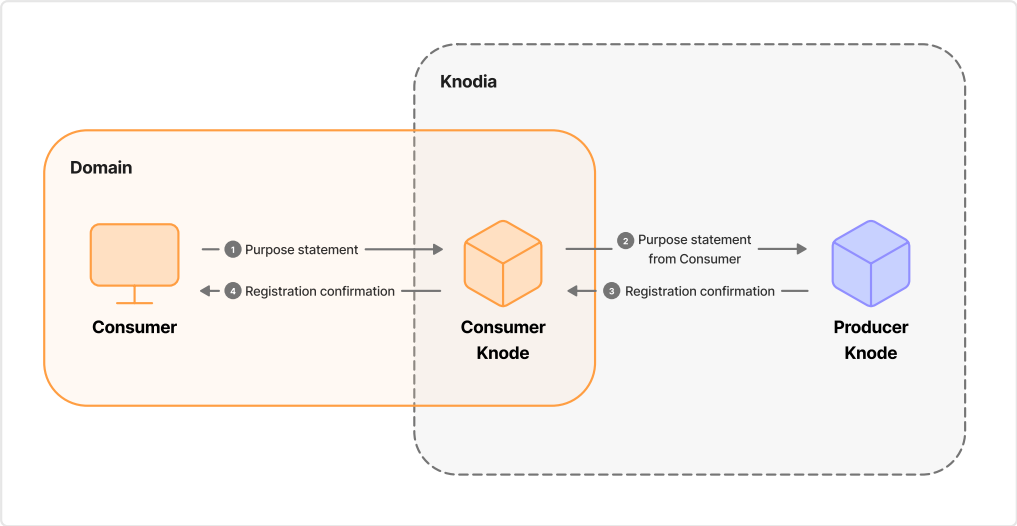


The *Producer Knode* can request additional information from the *Consumer* to implement the national regulatory framework (see § 5.5.3 “Actions requested by the national regulatory framework”). In this case, the *Consumer* may need to interact directly with the *Producer Knode*.

5.1.1.4 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*.

See § 5.5.2 “Purpose Statement” for details.

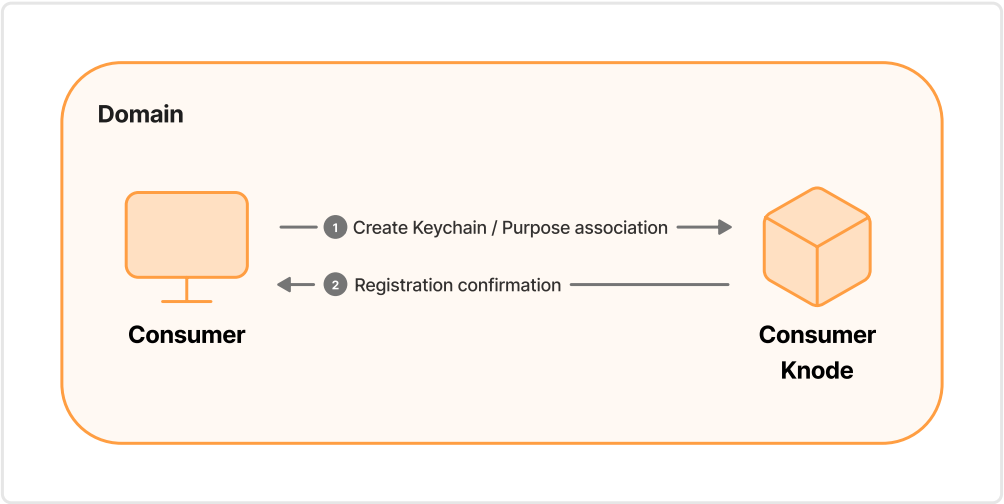


The *Producer Knode* can request additional information from the *Consumer* to implement the national regulatory framework regarding the protection of personal data of natural persons (see § 5.5.3 "Actions requested by the national regulatory framework"). In this case, the *Consumer* may need to interact directly with the *Producer Knode*.

5.1.1.5 Keychain association

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

See § 5.6.3 "Consumer Keychain association with Purpose Statements" for details.



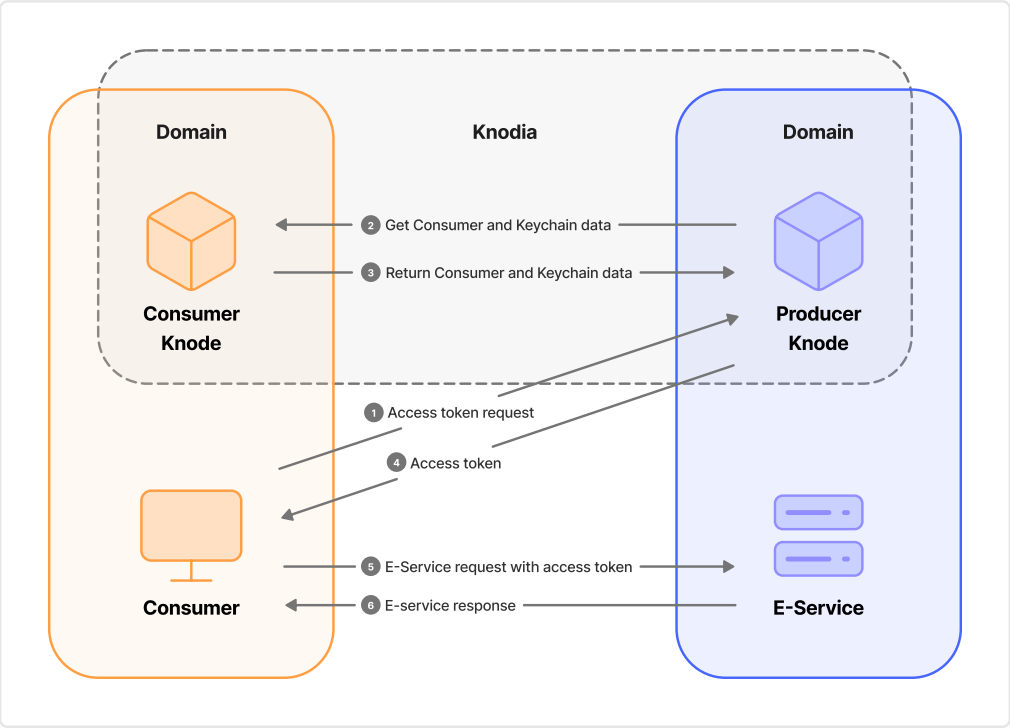
5.1.1.6 Access to a Cross-Border E-Service

The information that the *Producer Knode* has received and *Electronically Archived* in the steps described up to now constitutes the technical-administrative prerequisites that enable 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 *access token* issued by the *Producer Knode*.
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*.

See § 5.7 “Issuance of access tokens for Cross-Border E-Services” for details.



5.2 Management of Confederate Organizations

This section describes what *Knodes* must ensure regarding management of their own *Confederate Organizations*. Each *Knode* and its *Confederate Organizations* constitute, in compliance with specific legislation and regulation, a *Knodia Domain* based on mutual trust.

Knodes ensure certain identification of the *Confederate Organizations*. Each *Knode* defines the onboarding process and the required checks autonomously to constantly ensure that the prerequisites needed for enrollment of a *Confederate Organization* are met.

Knodia does not constrain how the onboarding process is implemented by *Knodes*, except that they must ensure that a single public or private subject can be onboarded only on a single *Knode*.

***Knodes* must ensure the following requirements are met:**

- **The manager of a *Knode* is responsible for the certain identification of *Confederate Organizations*, in accordance with the applicable regulatory framework.**
- **A public or private subject may be onboarded only on a single *Knode*.**

5.2.1 Attributes of Confederate Organizations

Attributes are characteristics that a *Confederate Organization* may have that determine which *Cross-Border E-Services* it can submit *Agreement Requests* for. This implements the ABAC (attribute-based access control) model, where:

- *Cross-Border E-Services* are the resources subject to access control, access meaning the right to submit an *Agreement Request*.
- The *Producer* specifies in the *consumption requirements* of its *Cross-Border E-Service* which *Attributes* are required.
- To submit an *Agreement Request* for the *Cross-Border E-Service*, a *Consumer* must possess the *Attributes* indicated by the *Producer* in the *consumption requirements*.

Knodia requires *Knodes* to manage *Attributes* for their *Confederate Organizations*.

Each *Knodia Domain* that joins *Knodia* must ensure that its *Knode* assigns and maintains *Attributes* that are shared among *Knodia*, hereinafter referred to as *Knodia Attributes*.

For example, consider that attributes are needed to identify the administrative divisions of Member States (NUTS). Each *Knode* should translate these attributes as befits its *Knodia Domain*: e.g., NUTS 1 should be translated as “Land” for Germany, NUTS 2 as “Regione” for Italy, etc.

Knodia must therefore define and share a controlled vocabulary for *Knodia Attributes*. In this example, this controlled vocabulary will contain the attributes “NUTS 1” and “NUTS 2” to identify the first- and second-level administrative divisions. Each *Knode* can render the *Knodia Attributes* translated into the languages of its *Knodia Domain*.

The lifecycle of this controlled vocabulary is a responsibility of the *Knodia Consortium*, as reported in § 5.11 "Considerations on the governance of Knodia".

***Knodes* must ensure the following requirements are met:**

- ***Knodes* must associate *Knodia Attributes* with *Confederate Organizations* in compliance with their reference regulatory framework.**
- ***Confederate Organizations* must not be able to modify their assigned *Knodia Attributes* on their own.**
- **Only *Knodia Attributes*, defined in the controlled vocabulary, are considered in *Knodia*.**

5.2.2 Management of Operators

Knodia does not constrain how *Knodia Domains* manage users that act on behalf of a *Confederate Organization*, hereinafter referred to as *Operators*. The only requirement is that, for each *Confederate Organization*, at least one *Operator* must exist with the required authorization to perform the tasks for that *Confederate Organization* within *Knodia* (publishing *Cross-Border E-Services*, managing *Agreement Requests* and *Purpose Statements*, etc.).

Knodia favours interactions between *Operators* and the *Knode* to which their *Confederate Organization* is onboarded. It minimizes direct interaction between *Operators* and the user interface of other *Knodes*.

Despite this, direct interaction between a *Consumer Operator* and a *Producer Knode* may be required. For this reason, *Operators* must possess means of electronic identification issued within an electronic identification scheme (hereinafter *eIDAS login*) notified pursuant to **Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC** (*eIDAS Regulation*).

***Knodes* must ensure the following requirements are met:**

- **For each *Confederate Organization*, at least one *Operator* must exist with the required authorization to perform the tasks for that *Confederate Organization* within *Knodia*.**
- **The *Operators* of *Confederate Organizations* that perform the tasks needed for *cross-border interactions* must possess *eIDAS logins*.**
- ***Operators* must be able to log in with eIDAS on the user interface of *Knodes* other than their own.**

5.3 Cross-Border E-Services

A *Cross-Border E-Service* is a Web service provided by a *Producer*, that is, published by it in the *Knode Catalogue* of the *Knode* to which the *Producer* has onboarded.

Producers publish *Cross-Border E-Services* so that other *Confederate Organizations* can access them, acting as *Consumers*.

Within *Knodia*, *Cross-Border E-Services* are assumed to use Hypertext Transfer Protocol Secure (HTTPS) as the communication protocol.

***Knodes* must ensure the following requirement is met:**

- **Whatever specificity their *Knodia Domain* has must not compromise the possibility of consuming *Cross-Border E-Services* with *cross-border interactions*.**

5.3.1 Technical characteristics

Cross-Border E-Services within *Knodia* are characterized by:

- An identifier which is unique within the *Knodia Domain*.
- A formal description of the application programming interface (hereinafter API), specified in an interface description language recognized in *Knodia* (for example, an OpenAPI specification for HTTP APIs).
- The duration and audience to be used by the *Knode* when issuing *access tokens* to *Consumers*.
- The quotas set by the *Producer* defining the maximum number of requests in a given unit of time:
  - Total maximum cross-border requests.
  - Total maximum cross-border requests from a single *Knode*.
  - Total maximum cross-border requests from a single *Consumer*.
- The mode of data transmission:
  - From the *Producer* to the *Consumer* (hereinafter *Provide-Data*).
  - From the *Consumer* to the *Producer* (hereinafter *Receive-Data*).
- Whether, to submit *Agreement Requests* and *Purpose Statements* for the *Cross-Border E-Service*, the *Consumer Operator* must confirm the submission via *eIDAS login* to the *Producer Knode*.
- Whether *Consumers* can access the *Producer Knode*'s Signal Hub functionality for this *E-Service* (for details, see § 5.10.2 "Distribution of data change signals (Signal Hub)").

***Knodes* must ensure the following requirement is met:**

- **Published *Cross-Border E-Services* ensure the indicated technical characteristics.**

5.3.2 Consumption requirements

Producers must associate *consumption requirements* with each *Cross-Border E-Service* to specify which *Knodia Attributes*, or combinations thereof, a potential *Consumer* must possess to submit an *Agreement Request* for the *E-Service*.

***Knodes* must ensure the following requirement is met:**

- **Published *Cross-Border E-Services* have associated *consumption requirements* defined in terms of *Knodia Attributes*.**

5.3.3 Metadata

Producers associate with *Cross-Border E-Services* metadata that is useful to present to *Operators* of other *Confederate Organizations*. These include, by way of non-exhaustive example, the name, description, and any additional documentation. The metadata must be provided at least in the common language accepted by *Knodia*.

***Knodes* must ensure the following requirement is met:**

- **Published *Cross-Border E-Services* include the metadata required by *Knodia* at least in its accepted common language.**

5.3.4 Knodia Categories

Knodes must allow *Producers* to associate *Cross-Border E-Services* with categories shared within *Knodia* (hereinafter *Knodia Categories*).This is intended to simplify service search by using standardized categories across all *Knodia Domains*.

By way of example, consider the need to identify the *Cross-Border E-Services* that provide data on a citizen's main address of residence. Several *Knodes* will include *E-Services* that provide this data, and *Knodes* can translate this concept as relevant in each *Knodia Domain*: "residenza" for Italy, "Wohnsitz" for Germany, etc.

Knodia must therefore define and share a controlled vocabulary for *Knodia Categories*. In this example, this controlled vocabulary will contain the category "main address" to identify this concept. Each *Knode* can render the *Knodia Attributes* translated into the languages of its *Knodia Domain*.

The lifecycle of this controlled vocabulary is a responsibility of the *Knodia Consortium*, as reported in § 5.11 "Considerations on the governance of Knodia".

***Knodes* must ensure the following requirement is met:**

- ***Cross-Border E-Services* can be associated with *Knodia Categories* and are preferably associated with at least one *Knodia Category*.**

5.4 Knode Catalogue

This section describes the functionality that *Knodes* must provide to their *Confederate Organizations* regarding the *Knode Catalogue*.

5.4.1 Cross-Border E-Service publication

A *Knode* must allow its *Confederate Organizations* that are *Producers* of *Cross-Border E-Services* to publish their *E-Services* on the *Knode Catalogue*.

To publish a *Cross-Border E-Service*, a *Producer* must define its required characteristics as described in § 5.3 “Cross-Border E-Services”. It must then manage its lifecycle as described in § 5.9.1 “Lifecycle of Cross-Border E-Services”.

Knodia does not prevent *Knodia Domains* from defining additional activities for these workflows, provided that any additions do not compromise the usability of the *Cross-Border E-Service* for *cross-border interactions*.

Knodes must ensure the following requirements are met:

- *Producers* have the tools needed to publish and manage the lifecycle of the *Cross-Border E-Services* they produce.
- Any additional activity specific to the individual *Knodia Domain* must not compromise the usability of the *Cross-Border E-Service* for *cross-border interactions*.

The following service blueprint outlines the activities performed by a *Producer Operator* on its *Producer Knode* to publish a *Cross-Border E-Service*. See § 6.2 “Reading service blueprints” for an explanation of the conventions used.

5.4.2 Cross-Border E-Service discovery

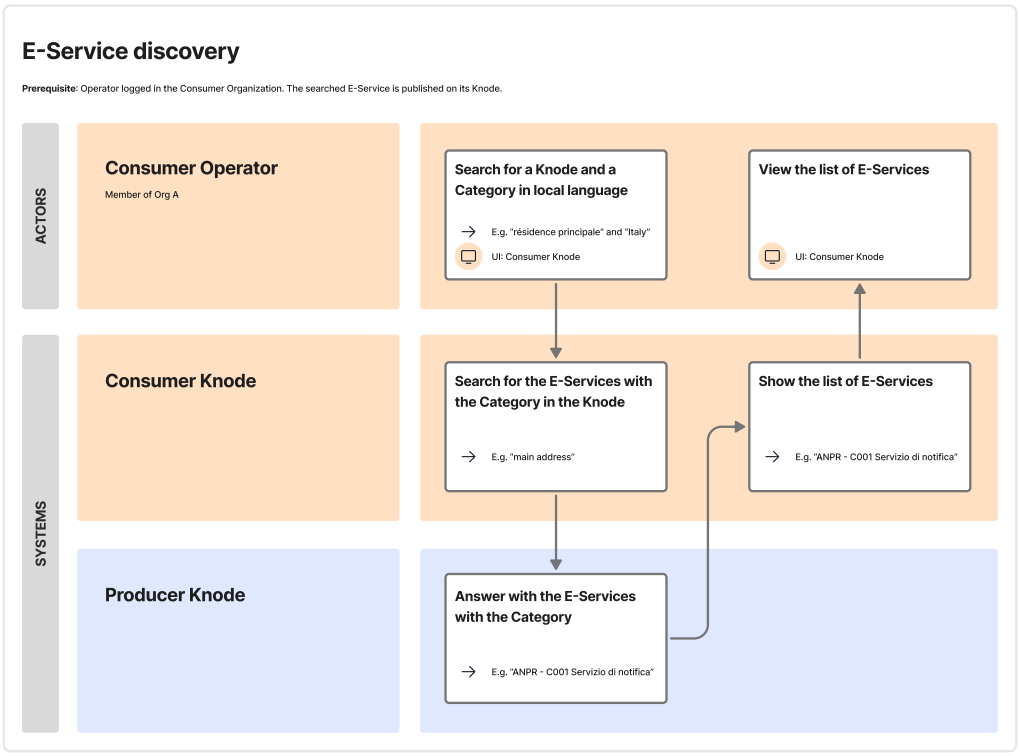
A potential *Consumer* can search for published *Cross-Border E-Services* through the user interface of their *Consumer Knode*. The user interface of every *Knode* must allow *Operators* of potential *Consumers* to:

- View the *Cross-Border E-Services* provided by a specific *Producer Knode* of interest to the *Consumer*, different from the *Consumer Knode*.
- Filter the list of *Cross-Border E-Services* by *Knodia Category* (for example, "main address", to search for *Cross-Border E-Services* that provide data on the main address of residence for citizens in the *Knodia Domain* represented by the *Producer Knode*).

The *Consumer Knode* must fetch the *Knode Catalogue* data on demand from the

Producer Knode using the machine-to-machine API defined within *Knodia* and implemented by each *Knode* (hereinafter *Knodia API*). See § 5.11.1 “Distribution of knowledge between Knodes” for details.

The following service blueprint outlines the activities performed by the subjects (*Operators* and *Knodes*) to search for a *Cross-Border E-Service*.



***Consumers Knodes* must ensure the following requirements are met:**

- ***Operators* of *Confederate Organizations* can view the *Cross-Border E-Services* of other *Knodes*.**
- ***Operators* of *Confederate Organizations* can filter the *Cross-Border E-Services* of other *Knodes* by *Knodia Category*.**
- **The data to display for each *Cross-Border E-Service* is fetched using the *Knodia API* from the corresponding *Knode*.**

***Producer Knodes* must ensure the following requirement is met:**

- **Published *Cross-Border E-Services* are made available to other *Knodes* via the *Knodia API*.**

5.5 Consuming Cross-Border E-Services

This section describes the functionality that *Knodes* must provide to their *Confederate Organizations* concerning *Agreement Requests* and *Purpose Statements* that allow *Consumers* in *Knodia* to consume *Cross-Border E-Services*.

As a whole, the actions described below and the information that is *Electronically Archived* by the interested parties digitally constitute an interoperability agreement between *Producer* and *Consumer*, as defined by the *EIF*.

The section also describes the difference between the two modes of data transmission for *Cross-Border E-Services*:

- *Provide-Data*, in the case where the *Producer* sends data to the *Consumer*.
- *Receive-Data*, in the case where the *Producer* receives data from the *Consumer*.

5.5.1 Agreement Request

An *Agreement Request* is a digital agreement between a *Consumer* and a *Producer* regarding a *Cross-Border E-Service* produced by the *Producer*. The *Agreement Request* is needed for the *Consumer* to consume the *E-Service*.

For *Provide-Data Cross-Border E-Services*, the *Agreement Request* is not sufficient to allow usage of the *E-Service*, since the *Consumer* must also submit the *Purpose Statement* (see § 5.5.2 “Purpose Statement” for more details).

The *Consumer*, after identifying the *Cross-Border E-Service* it intends to consume, can submit an *Agreement Request* for it via the *Consumer Knode* user interface. Using the *Knodia API*, the *Consumer Knode* forwards to the *Producer Knode*:

- The identifier of the *Cross-Border E-Service*.
- The identifier of the *Consumer* and its *Knodia Attributes*.

The *Producer Knode* can thus verify whether the *Consumer* satisfies the *consumption requirements* of the *Cross-Border E-Service*. If so, it creates an *Agreement Request*, *Stores* it, and sends its identifier to the *Producer Knode*.

By default, *Knodia* assumes that the *Producer Knode* will activate the *Agreement Request* when it creates it. The following service blueprint outlines the activities performed by the subjects in this case.

Activating an *Agreement Request* may require additional actions depending on the regulatory framework in which the *Producer Knode* operates; see § 5.5.3 “Actions requested by the national regulatory framework”.

The *Agreement Request* must be filled in at least in the common language accepted by *Knodia*.

The *Consumer Knode* must monitor state change events to the *Agreement Request* using the *Knodia API* and notify the corresponding *Consumer*. See § 5.11.1 “Distribution of knowledge between Knodes” for more details.

The *Consumer Knode* must *Store* the references (identifiers) of:

- The *Agreement Request*, as returned by the *Producer Knode*, so it can later fetch its details using the *Knodia API*.
- The *Cross-Border E-Service* involved in the *Agreement Request*.
- The *Producer Knode*.

The *Consumer Knode* must *Electronically Archive* the information on:

- The *Consumer*, including its *Knodia Attributes*.

The *Producer Knode* must *Electronically Archive* the information on:

- The *Agreement Request*.
- The *Cross-Border E-Service* involved in the *Agreement Request*.

The *Producer Knode* must *Store* the references (identifiers) of:

- The *Consumer*.
- The *Consumer Knode*.

Each *Producer Knode* must update the state of each *Agreement Request* it has created in response to:

- Changes to the *Cross-Border E-Service* originated by the Producer.
- Changes to the *Knodia Attributes* of the *Consumer*, obtained by monitoring events using the *Knodia API* of the *Consumer Knode* (see § 5.11.1 “Distribution of knowledge between Knodes” for more details).

Specifically, the *Agreement Request* must be suspended if the *Consumer*'s *Knodia Attributes* no longer satisfy the *consumption requirements* of the *Cross-Border E-Service*.

Within *Knodia*, for each *E-Service* and *Consumer*, there can be at most one *Agreement Request*.

See § 5.9.2 “Lifecycle of Agreement Requests” for more details on the lifecycle of *Agreement Requests*.

***Consumer Knodes* must ensure the following requirements are met:**

- ***Confederate Organizations* can submit *Agreement Requests* for *E-Services* and receive notifications concerning these *Agreement Requests*.**
- **The *Knode* uses the *Knodia API* of the *Producer Knode* to forward the request to create an *Agreement Request*.**
- **The Knode uses the *Knodia API* to receive evidence from the *Producer Knode* about the state of the created *Agreement Requests*.**
- **Changes in the *Knodia Attributes* of *Confederate Organizations* are made available to *Producer Knodes* via the *Knodia API*.**

***Producer Knodes* must ensure the following requirements are met:**

- ***Consumer Knode* can submit an *Agreement Request* using the *Knodia API*.**
- **The state of the *Agreement Request* is kept up to date.**
- **Changes in the state of *Agreement Requests* are made available to the *Consumer Knodes* that created them via the *Knodia API*.**

5.5.1.1 Confirmation by the Consumer Operator

The *Producer* can optionally configure the *Cross-Border E-Service* to request an *Operator* of the *Consumer* to confirm the submission of an *Agreement Request* on the *Producer Knode*.

This allows the *Producer Knode* to *Electronically Archive*, for an *Agreement Request*, the explicit confirmation of an *Operator* of the *Consumer*, together with the request received from the *Consumer Knode*.

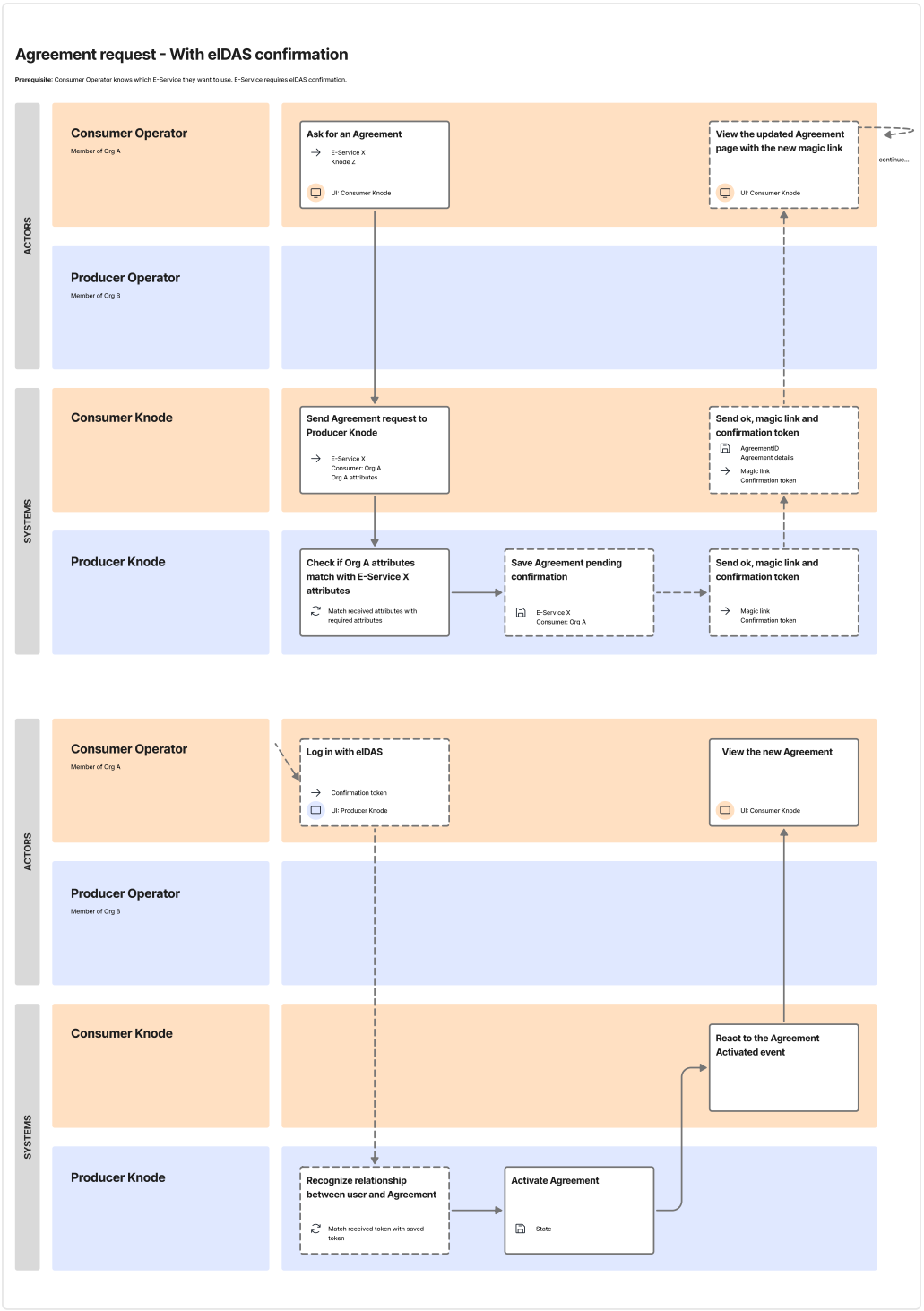
In this case, when the *Producer Knode* creates the *Agreement Request*, it must send to the *Consumer Knode* (together with the identifier of the *Agreement Request*):

- A link to its user interface that a *Consumer Operator* must use to confirm the operation on the *Producer Knode*.
- An (unforgeable) secret token that the aforementioned *Operator* must provide to the *Producer Knode*.

To confirm submission of an *Agreement Request*, an *Operator* of the *Consumer* must follow the link, authenticate to the *Producer Knode* user interface via *eIDAS login*, and provide the secret token.

The *Consumer Knode* is responsible for providing the link and secret token only to the *Operators* of the *Consumer* who are authorized in its domain to perform this confirmation.

After confirmation, if no other action is needed, the *Producer Knode* activates the *Agreement Request*. This case is illustrated in the following service blueprint.



If the regulatory framework applicable to the *Producer Knode* requires additional actions, the *Producer Knode* sets the *Agreement Request* state accordingly (see § 5.5.3 “Actions requested by the national regulatory framework”).

***Producer Knodes* must ensure the following requirements are met:**

- ***Producers* can request explicit confirmation from potential *Consumers* before activating their *Agreement Requests*.**
- **If a *Producer* requests explicit confirmation, the *Producer Knode* returns to interested *Consumer Knodes*, via the *Knodia API*, the information needed for *Operators* to fulfil this.**

***Consumers Knodes* must ensure the following requirements are met:**

- **The *Consumer Knode* must monitor state changes in the *Agreement Request* using the *Knodia API* to detect when confirmation has occurred.**
- **The *Consumer Knode* must forward to interested consumers the information needed to fulfil the *Producer*'s explicit confirmation request, received from the *Producer Knode*.**

5.5.2 Purpose Statement

A *Purpose Statement* is the declaration a *Confederate Organization* makes to assert the lawfulness of processing of personal data received through a *Cross-Border E-Service*, pursuant to Article 6 of the *GDPR*.

A *Purpose Statement* is necessary to enable the *Consumer* to access a *Cross-Border E-Service*, even if the *Producer* has declared that the *Cross-Border E-Service* does not provide or process personal data of natural persons.

This declaration is made:

- For *Provide-Data Cross-Border E-Services*, by the *Consumers*, for each *E-Service* they have an active *Agreement Request* for, and each data processing purpose they will apply on the *E-Service* data.
- For *Receive-Data Cross-Border E-Services*, by the *Producer* when publishing the *E-Service*.

Within *Knodia*, *Purpose Statements* are characterized by:

- An identifier which is unique within the *Knodia Domain*.
- Name and description.
- Indication of the lawfulness of processing, as a value chosen from the options admitted by Article 6 of Regulation (EU) 2016/679.
- Any additional information required by the national regulatory framework to which the *Producer Knode* is subject regarding the protection of personal data of natural persons (see § 5.5.3 "Actions requested by the national regulatory framework").

The *Purpose Statements* must be filled in at least in the common language accepted by *Knodia*.

The *Consumer* must declare the load it expects to place on the *Cross-Border E-Service*, expressed as a maximum number of requests per unit of time. This parameter is useful to the *Producer* to evaluate the dimensioning of its technological infrastructure. Specifically:

- For *Provide-Data E-Services*, the *Consumer* declares it in each *Purpose Statement* it creates.
- For *Receive-Data E-Services*, the *Consumer* declares it by selecting the *Purpose Statement* created by the *Producer*.

Each *Producer Knode* may choose to define and perform checks comparing the load declared by the *Consumer* to the quotas defined by the *Producer* of the *Cross-Border E-Service*. For example, a *Knode* may choose:

- Not to perform any check (the load declaration is only used to inform the *Producer*, who can dimension infrastructure accordingly and possibly defer or reject requests in excess of the declared load).
- To prevent the creation of new *Purpose Statements* if existing *Purpose Statements* saturate the quotas declared by the *Producer* for that *E-Service*.

See § 5.9.3 "Lifecycle of Purpose Statements" for more details on the lifecycle of *Purpose Statements*.

***Consumer Knodes* must ensure the following requirements are met:**

- ***Confederate Organizations* can create or select (respectively, for *Provide-Data* or *Receive-Data Cross-Border E-Services*) the *Purpose Statements* for *Cross-Border E-Services* and receive notifications related to them.**
- **The *Consumer Knode* must forward the request to create a *Purpose Statement* to the *Producer Knode* using the *Knodia API*.**
- **The *Consumer Knode* must receive from the *Producer Knode*, using the *Knodia API*, evidence on the state of *Purpose Statements* it has created.**

***Producer Knodes* must ensure the following requirements are met:**

- **The *Producer Knode* must allow other *Knodes* to create *Purpose Statements* (for *Provide-Data Cross-Border E-Services*) or to retrieve existing *Purpose Statements* created by the *Producer* (for *Receive-Data Cross-Border E-Services*) using the *Knodia API*.**
- **Changes in the state of *Purpose Statements* are made available to the *Consumer Knodes* that created them via the *Knodia API*.**

5.5.2.1 Purpose Statements for Provide-Data E-Services

A *Consumer Operator* may, through the user interface of the *Consumer Knode*, make one or more *Purpose Statements* related to a *Cross-Border E-Service* for which it has an active *Agreement Request*.

The *Consumer Knode*:

1. Requests to the *Consumer Operator* to fill in the required information according to the requirements defined in the § 5.5.2 "Purpose Statement" above.
2. Retrieves from the *Producer Knode*, using the *Knodia API*, the form for any additional information requested by the national regulatory framework (see § 5.5.3 "Actions requested by the national regulatory framework" for details).

3. Provides the form to the *Consumer Operator* to fill in.
4. Forwards the filled-in data to the *Producer Knode* using the *Knodia API*.

The *Producer Knode* creates the *Purpose Statement* and returns its reference to the *Consumer Knode*.

The *Consumer Knodes* must *Store* the references:

- Of the *Purpose Statement*, as returned by the *Producer Knode*, to be able to retrieve its data later using the *Knodia API*.
- Of the *Cross-Border E-Service* subject of the declaration.
- Of the *Producer Knode*.

The *Consumer Knode* must *Electronically Archive* the information:

- On the *Consumer*, including its *Knodia Attributes*.

The *Producer Knode* must *Electronically Archive* the information:

- Of the *Purpose Declaration*.
- Of the *Cross-Border E-Service* subject of the declaration.

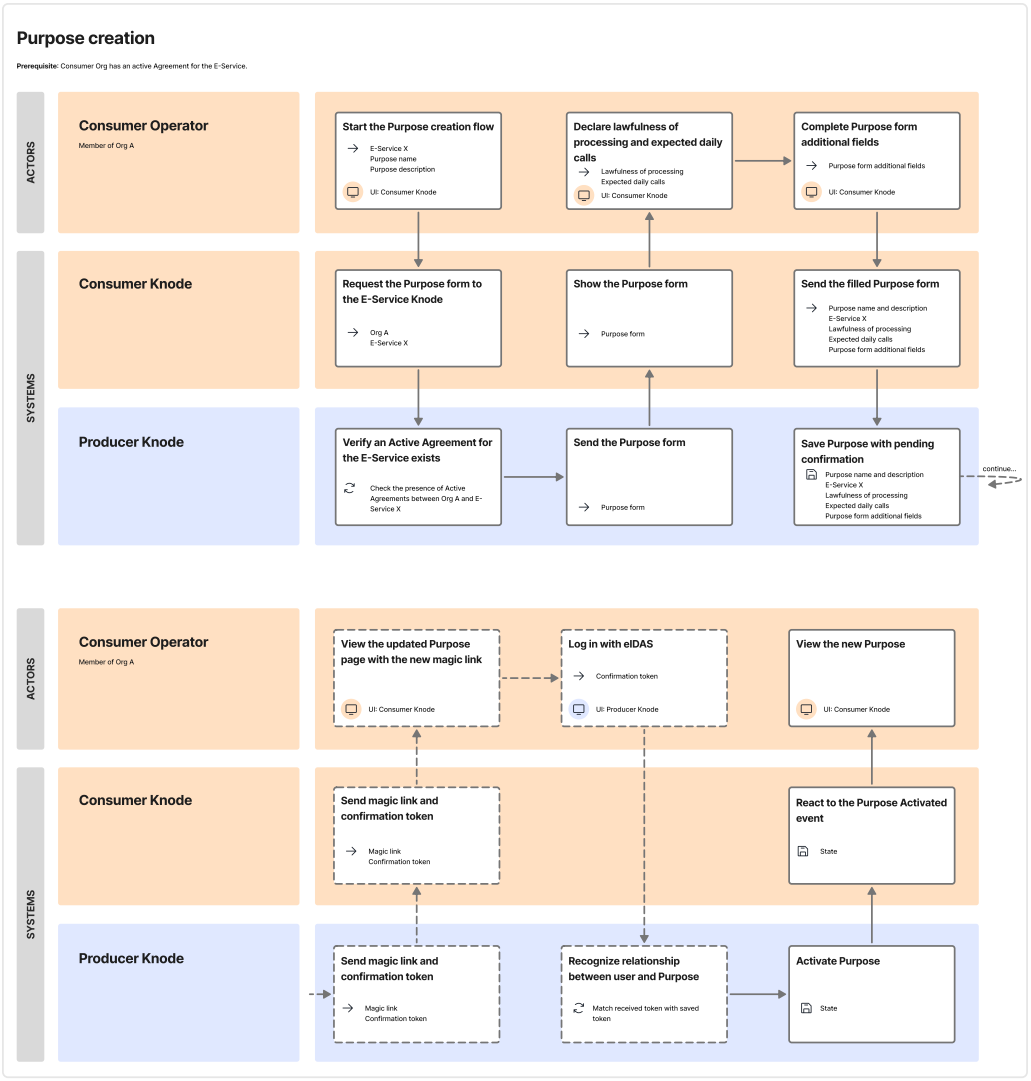
The *Producer Knode* must *Store* the references:

- Of the *Consumer*.
- Of the *Consumer Knode*.

The default behaviour in *Knodia* is for the *Producer Knode* to activate the *Purpose Declaration* simultaneously when it is created.

The *Purpose Statement* may instead need further confirmation by a *Consumer Operator* if the *Producer* requested it when creating the *Cross-Border E-Service*. In this case, the procedure is equivalent to that described for confirmation of *Agreement Requests* (see § 5.5.1.1 “Agreement Request – Confirmation by the Consumer Operator”).

The following service blueprint outlines the activities performed by the subjects (*Operators* and *Knodes*) in the latter case.



In any case, the *Consumer Knode* must monitor state change events for the *Purpose Statement* using the *Knodia API* and notify the corresponding *Consumer*. See § 5.11.1 “Distribution of knowledge between Knodes” for more details.

***Producer Knodes* must ensure the following requirements are met:**

- ***Producers* can request explicit confirmation from potential *Consumers* before activating their *Agreement Requests*.**
- **If a *Producer* requests explicit confirmation, the *Producer Knode* returns to interested *Consumer Knodes*, via the *Knodia API*, the information needed for *Operators* to fulfil this.**
- **If any additional information is requested from the *Consumer* in relation to the regulation for protection of personal data of natural persons, the *Producer Knode* must provide interested *Consumer Knodes*, through the *Knodia API*, with the form to collect this information and the operations to receive it after it is completed.**

***Consumer Knodes* must ensure the following requirements are met:**

- ***Consumer Knodes* must monitor, using the *Knodia API* of the *Producer Knodes*, state changes of *Purpose Statements*, to react when the confirmation is given.**
- **If any additional information is requested from the *Consumer* in relation to the regulation for protection of personal data of natural persons, the *Consumer Knode* must retrieve the form to collect this information and forward it to the *Producer Knode*.**

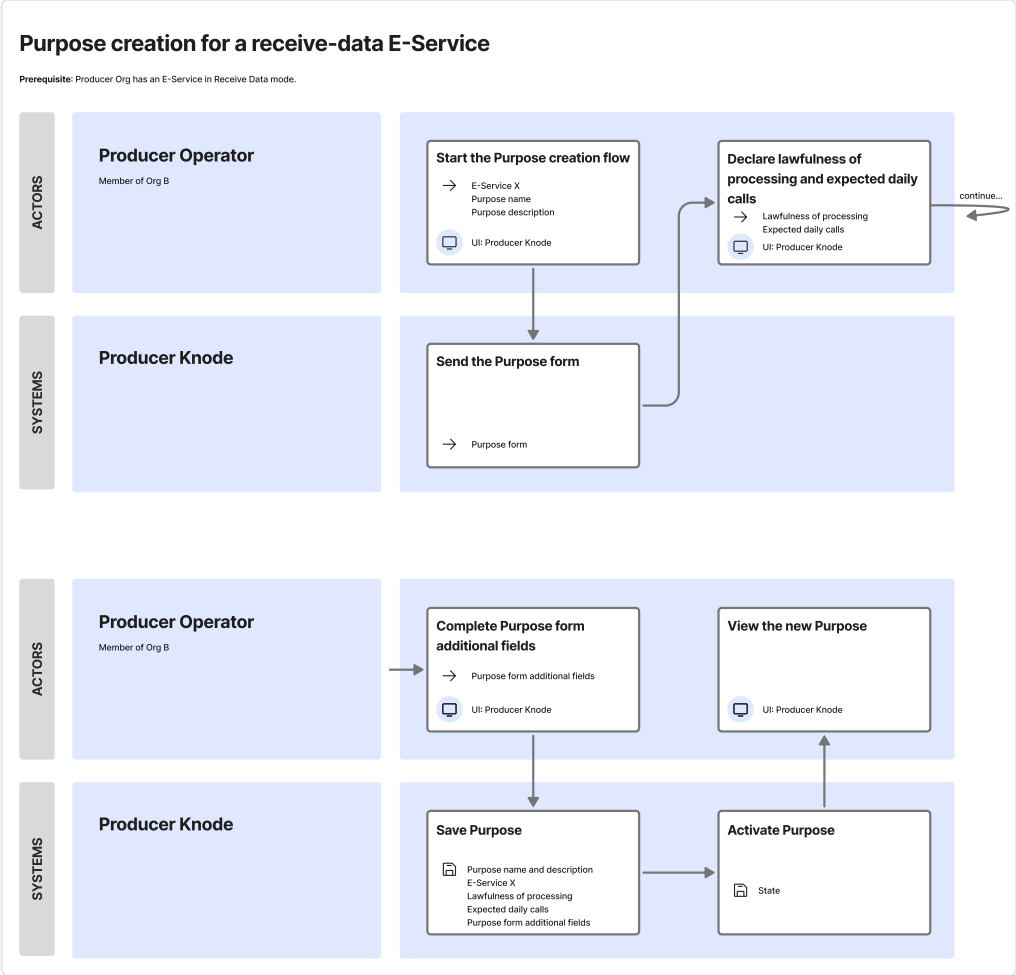
5.5.2.2 Purpose Statements for Receive-Data E-Services

A *Cross-Border E-Service* in the *Receive-Data* mode allows its *Producer* to collect data from *Consumers*. In this case, the *Purpose Statement* must be issued by the *Producer*, the subject that processes the data.

The *Producer Knode* must provide functionality for *Producers* to enter the required information in accordance with the requirements defined in the § 5.5.2 “Purpose Statement” above.

The *Consumer Knode*, when a *Consumer* has an active *Agreement Request* for a *Receive-Data Cross-Border E-Service*, must retrieve from the *Producer Knode*, using the *Knodia API*, the *Purpose Statements* and make them available to the *Consumer*.

The following service blueprint illustrates the flow of activities for purpose creation in the *Receive-Data* case:



***Consumer Knodes* must ensure the following requirement is met:**

- **They must retrieve the *Purpose Statement* issued by the *Producer*, using the *Knodia API*, and make it available to the *Consumer* on their user interface.**

***Producer Knodes* must ensure the following requirement is met:**

- **They must make the *Purpose Statement* issued by the *Producer* available through the *Knodia API* to *Consumer Knodes*.**

5.5.3 Actions requested by the national regulatory framework

5.5.3.1 Additional actions for Agreement Requests

As mentioned in § 5.5.1 “Agreement Request”, additional actions may be needed to activate an *Agreement Request*. This is at the discretion of the *Producer Knode*. It makes it possible for *Knodes* to implement any additional steps demanded by the national regulatory framework they are subject to: for example, request additional information from the *Consumer* to complete the proceedings.

For this reason, after the the *Consumer* submits the *Agreement Request*, the *Consumer Knode* must monitor state change events for the *Agreement Request* using the *Knodia API*. See § 5.11.1 “Distribution of knowledge between Knodes” for more details.

Before the *Agreement Request* reaches the active state, it can transit through one or more of these states:

- Additional action requested from a *Producer Operator*, e.g., manual approval.
- Additional action requested from a *Consumer Operator*.

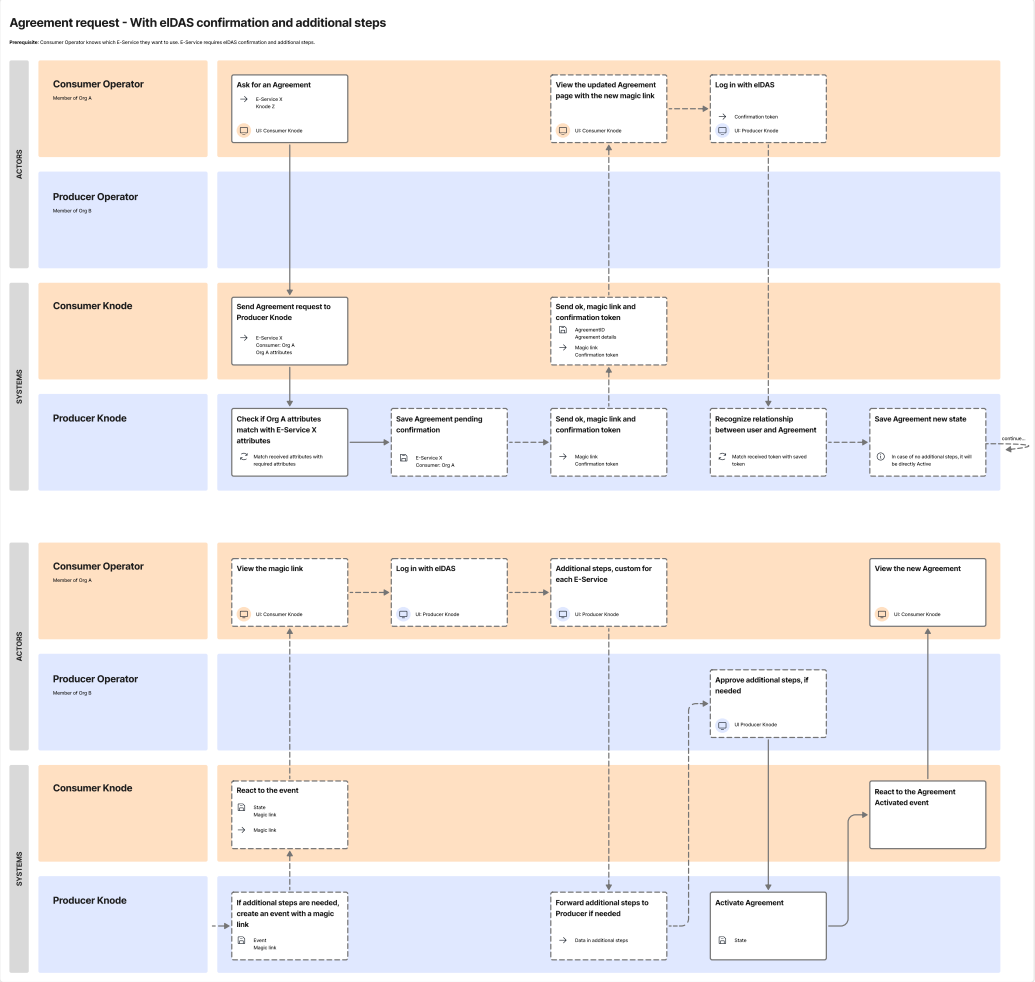
The first case is managed internally to the *Producer Knode*.

In the second case, the *Producer Knode* must include, in the state change event, a link and any additional elements needed for the *Consumer* to perform the requested actions.

When the *Producer Knode* forwards such a link, it must ensure that its user interface supports at least the common language accepted by *Knodia*.

When the *Consumer Knode* receives the link and any additional elements, it must provide them to *Consumer Operators* so they can perform the requested actions.

The following service blueprint outlines the activities performed by the subjects (*Operators* and *Knodes*) in this case.



***Producer Knodes* must ensure the following requirement is met:**

- **If additional actions are needed by the *Consumer*, they must notify the interested *Consumer Knode* using the *Knodia API*, including the link and any additional elements needed to perform the requested actions.**

***Consumer Knodes* must ensure the following requirements are met:**

- **They must retrieve from the *Producer Knode*, using the *Knodia API*, the link and any additional elements needed to perform the requested actions.**
- **They must forward the link and any additional elements received from the *Producer Knode* to the *Consumer*.**

5.5.3.2 Additional information for Purpose Statements

As mentioned in § 5.5.2 “Purpose Statement”, additional information beyond the default may be needed for the *Purpose Statement*. This is at the discretion of the *Producer Knode*, to comply with the national regulatory framework they are subject to.

This request for additional information is made through a custom form defined by the

Producer Knode. See § 5.5.2 "Purpose Statement" for the service blueprint and the description of how this form is transmitted between *Knodes* when the statement must be made by the *Consumer*.

This form:

- Must be defined following a format shared within *Knodia*, which supports multiple languages.
- Must be made available by the *Producer Knode* at least in the common language accepted by *Knodia*.
- Must accept responses in any of the languages it is made available in.

Defining the standard format that every *Knode* must use for the form is a responsibility of the *Knodia Consortium* mentioned in § 5.11.2 "Configuration of the federation of Knodes".

***Producer Knodes* must ensure the following requirements are met:**

- **They must use the standard format of *Knodia* to define the form that *Consumers* of *Cross-Border E-Services* must fill in.**
- **They must provide the form to *Consumer Knodes* using the *Knodia API*.**

***Consumer Knodes* must ensure the following requirements are met:**

- **They must retrieve the form from the *Producer Knode* using the *Knodia API*.**
- **They must require *Consumer Operators* to view and complete the form.**

5.6 Consumer Keychains

This section describes the functionality that every *Knode* must provide to *Confederate Organizations* regarding *Consumer Keychains*. These are needed for *Consumers* to use the *Knode*'s API to request *access tokens* to consume a *Cross-Border E-Service*.

5.6.1 Context of use

A *Consumer* who has an active *Agreement Request* and an active *Purpose Statement* for a *Cross-Border E-Service* has all the prerequisites to consume it. The *Producer Knode* can therefore issue *access tokens* which the *Consumer* can use to access the *E-Service*'s API.

The *Consumer* can request an *access token* using an API on the *Producer Knode*, referred to hereinafter as the token endpoint. Authentication of requests to the token endpoint (that is, verification that they originate from the IT system of the *Consumer* in *Knodia*) complies with the OAuth2 framework. Specifically, it requires the *Consumer* to prepare a client assertion, i.e., a JSON web token (JWT):

- Which is sealed with an Electronic Seal created using the private cryptographic material in the *Consumer*'s possession.

- Which contains the information needed for the *access token* request, outlined in § 5.7 “Issuance of access tokens for Cross-Border E-Services”.

The token endpoint authenticates the *Consumer* by verifying the signature of the client assertion using the *Consumer*'s public cryptographic material. Therefore, the *Consumer* must deposit the public cryptographic material in a dedicated keychain, the *Consumer Keychain*, so that the *Producer Knode* can access it.

5.6.2 Management of cryptographic material

The *Consumer Keychain* is the digital container in which the *Consumer* deposits the public cryptographic material corresponding to the *Electronic Seals* it uses to seal *access token* requests for consuming *Cross-Border E-Services*.

Each *Consumer* creates and manages its *Consumer Keychains* via the user interface on its *Consumer Knode*. The *Consumer Knode* must make *Consumer Keychains* available through the *Knodia API* so a *Producer Knode* can retrieve the cryptographic material needed for verification. See § 5.7 “Issuance of access tokens for Cross-Border E-Services” for more details.

This architectural choice lets each *Knode* be fully autonomous in managing the public cryptographic material of its onboarded *Confederate Organizations*. Therefore, this material does not need to be distributed across different nodes, which would be more complex and could increase the risk of misalignment.

The user interface of each *Consumer Knode* must enable *Consumer Operators* to:

- Create a *Consumer Keychain*.
- Deposit in the *Consumer Keychain* the aforementioned public cryptographic material (one or more public keys).

Knodes must support depositing X.509 certificates or public keys as public cryptographic material in *Consumer Keychains*.

The *Consumer Knode* must manage the lifecycle of the cryptographic material if the *Operator* that deposited it loses authorization rights within the *Confederate Organization* (for example, removing all keys deposited by an *Operator* who no longer has access to the *Confederate Organization*).

***Consumer Knodes* must ensure the following requirements are met:**

- **They must allow their *Confederate Organizations* to manage *Keychains*.**
- **They must make the public cryptographic material deposited by *Consumers* available to *Producer Knodes* through the *Knodia API*.**

***Producer Knodes* must ensure the following requirement is met:**

- **They must retrieve the *Consumers'* public cryptographic material from *Consumer Knodes* to verify the *Consumers' client assertions*.**

5.6.3 Consumer Keychain association with Purpose Statements

A *Consumer Keychain* can be used to consume multiple *Cross-Border E-Services*. To this end, the *Consumer Keychain* is associated with a set of active *Purpose Statements*.

The *Consumer Knode* user interface must allow *Consumer Operators* to associate the *Consumer Keychain* with one or more active *Purpose Statements*. For *Receive-Data Cross-Border E-Services*, the *Purpose Statement* associated with the *Consumer Keychain* is one that the *Producer* created when publishing the *Cross-Border E-Service* itself.

The association occurs via the identifiers of the *Purpose Statements* stored when they are created.

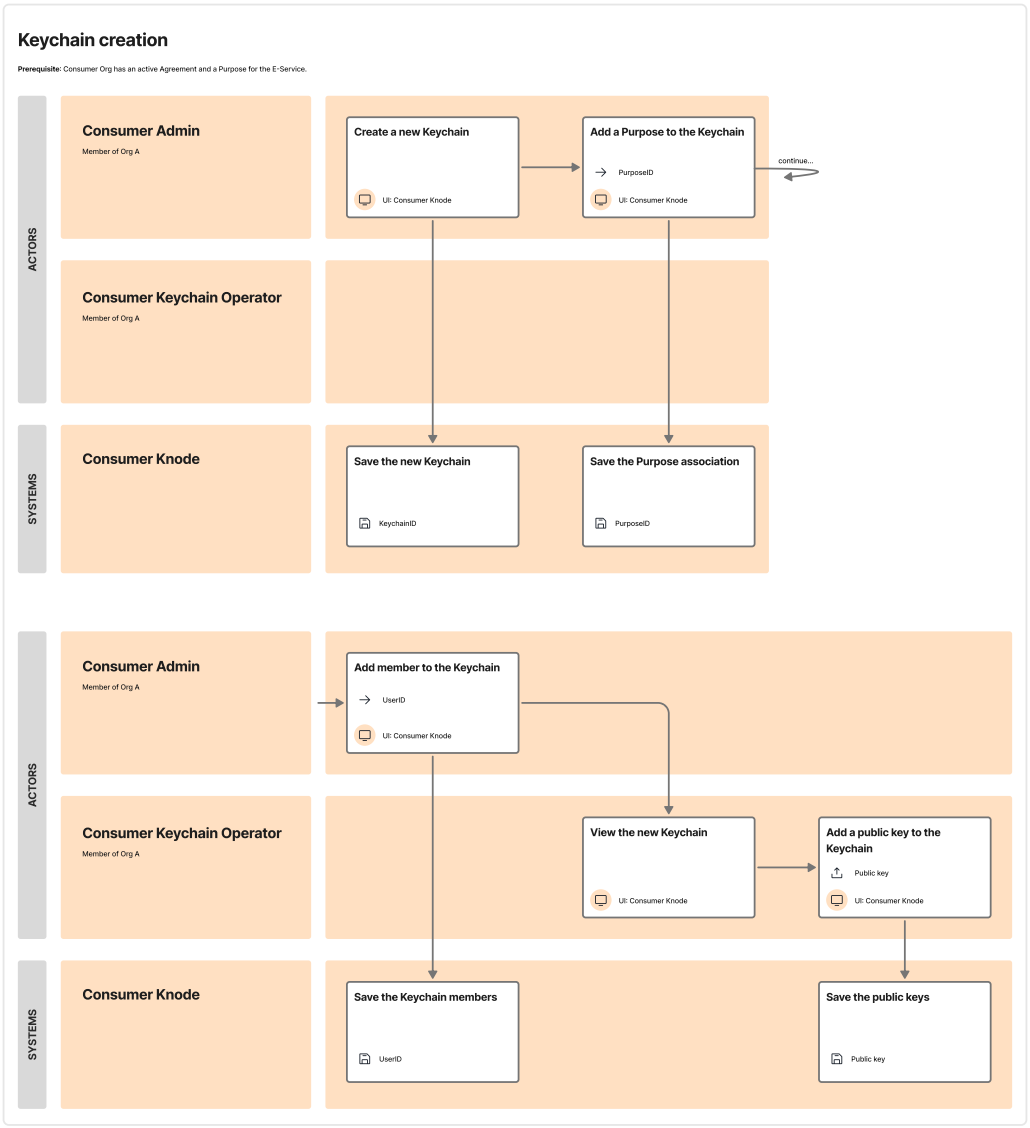
The *Consumer Keychain* can afterwards be used to request *access tokens* for the related *E-Services*.

***Consumer Knodes* must ensure the following requirement is met:**

- **They must let *Consumers* associate *Keychains* with *Purpose Statements*.**

The following service blueprint illustrates the flow in an example case in which the *Consumer Knode* has defined two distinct roles for its *Operators*. See § 5.2.2 “Management of Operators” for more details. This example considers two roles:

- Admin, who can create *Consumer* Keychains and associate them with *Operators* with the Keychain *Operator* role.
- Keychain Operator, who can deposit public cryptographic material.



5.7 Issuance of access tokens for Cross-Border E-Services

This section describes how *Knodes* can issue *access tokens* for *Cross-Border E-Services* of their *Producers* to *Consumers* of other *Knodes* in *Knodia*. *Access tokens* are issued only if there exists an active *Agreement Request* and at least one active *Purpose Statement* for that *Consumer*.

The type of *access token* required to access a specific *Cross-Border E-Service* is defined by the *Producer* when creating the *Cross-Border E-Service*. The *Consumer* must request an *access token* according to that type.

5.7.1 Bearer authorization

If the *Producer* has defined the *Cross-Border E-Service* as accepting Bearer authentication, the *Consumer* requests an *access token* by making a request to the token endpoint of the *Producer Knode*, attaching a client assertion as defined in § 5.6.1 “Consumer Keychains – Context of use”. The assertion must contain at least the following attributes:

- *sub* and *iss*: identifiers of the *Consumer* Keychain containing the public cryptographic material corresponding to the seal applied to the client assertion.
- *aud*: the audience defined when the *Cross-Border E-Services* was created.
- *purposeId*: the identifier of a *Purpose Statement* associated with the *Cross-Border E-Service* and the *Consumer Keychain*.
- *jti*: a random, unique identifier assigned by the *Consumer*.
- *iat*: the timestamp reporting the date and time the token is created.
- *exp*: the timestamp reporting the date and time of token expiration.

The *Producer Knode* follows these steps to issue the token:

1. Retrieve the needed information using the *Knodia API* of the *Consumer Knode*:
    - Data of the *Consumer Keychain*: public cryptographic material and associated *Purpose Statements*.
    - Data of the *Consumer* and its *Knodia Attributes*.
2. Authenticate the *Consumer*, that is, verify the seal of the client assertion against the public cryptographic material in the keychain.
3. Authorize, that is, verify:
    - That the *Purpose Statement* referred to in the client assertion is active and associated with the Keychain.
    - That there exists an active *Agreement Request* for the *Consumer* for that *Cross-Border E-Service*.
    - That the *Cross-Border E-Service* is in a state in which it can be consumed (see § 5.9.1 “Lifecycle of Cross-Border E-Services”).
    - That the *Consumer*'s *Knodia Attributes* satisfy the *consumption requirements* of the *Cross-Border E-Service*.

If verification succeeds, the *Producer Knode* creates and seals the *access token*, then returns it to the *Consumer*. The *Consumer* can then call the *Cross-Border E-Service* using the token as HTTP Authentication in Bearer mode.

The *Producer* is responsible for implementing *access token* verification in the *Cross-Border E-Service*. That is, it must verify that it is a valid JWT, with respect to expiration and audience, and that it is electronically sealed by the *Producer Knode* (which guarantees authenticity and integrity). To allow this, the *Producer Knode* must make its own public cryptographic material, with which it seals the *access tokens* it issues, publicly available as a well-known JSON Web Key Set (JWKS).

The implementation details of the token endpoint, which the *Producer Knodes* must implement, shall be part of the *Knodia* specification produced by the Federated Consortium, as described in § 5.11 “Considerations on the governance of Knodia”.

***Consumers* must ensure the following requirements are met:**

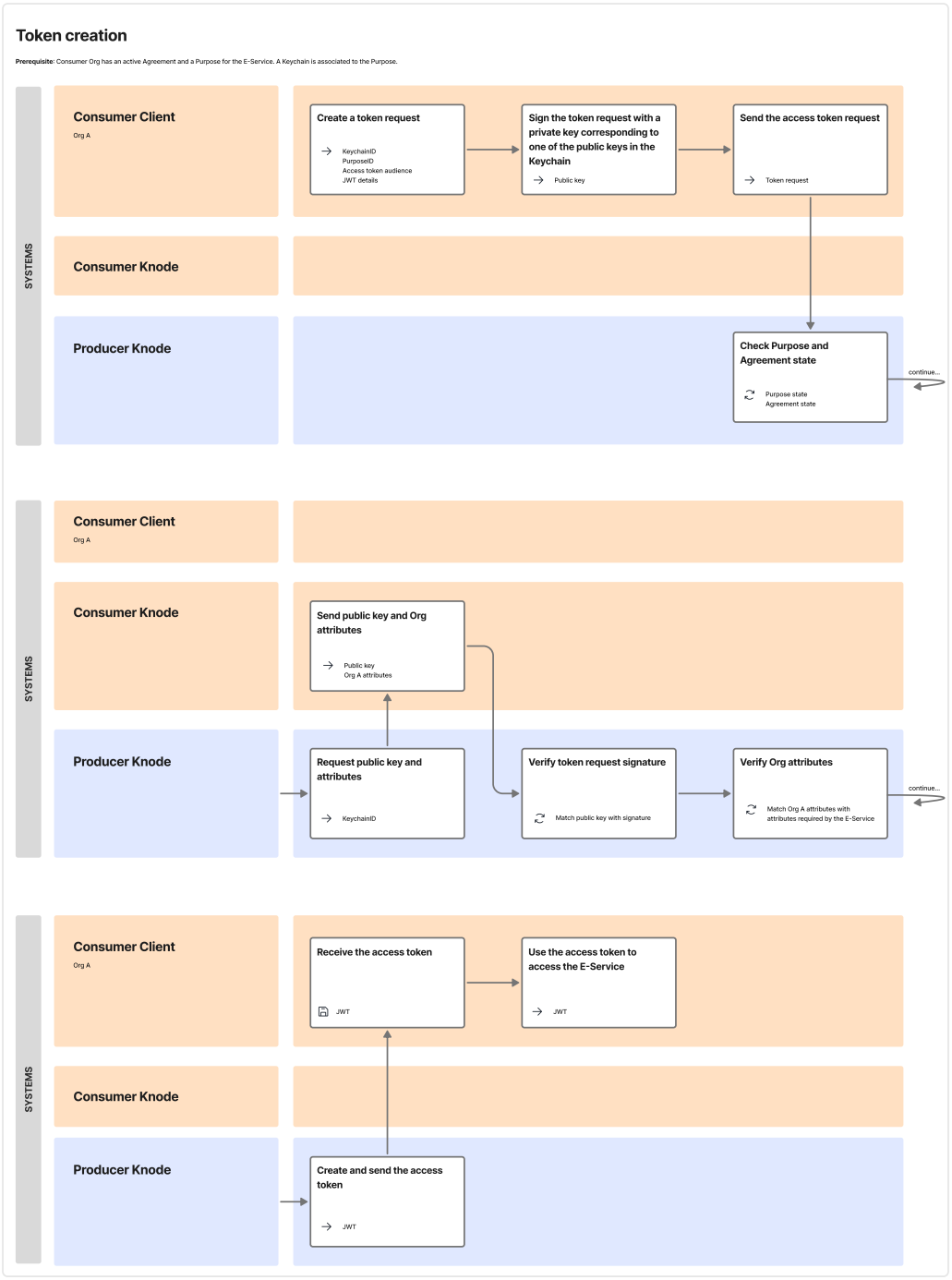
- **They must request an *access token* from the *Producer Knode* corresponding to the *Cross-Border E-Service* of interest and to a specific active *Purpose Statement*.**
- **They must use the *access token* issued by the *Producer Knode* to request access to the *Producer* for the *Cross-Border E-Service* of interest.**

***Producer Knodes* must ensure the following requirement is met:**

- **They must implement the token endpoint that issues *access tokens* in accordance with the *Knodia* specification and make it available to *Consumers*.**

***Producers* must ensure the following requirement is met:**

- **They must validate the *access token* sent by the *Consumer* before granting access to their *Cross-Border E-Service*.**



5.7.2 Authorization with proof of possession

Knodes must support Demonstrating Proof of Possession (hereinafter, *DPoP*) to strengthen the security of access to *Cross-Border E-Services*. *DPoP* requires *Consumers* to demonstrate to *Producers* that they possess their own private cryptographic material. This makes stolen *access tokens* unusable by unauthorized subjects.

The *Producer* can request *DPoP* to apply for a *Cross-Border E-Service* when it creates the *Cross-Border E-Service*. In this case, *Consumers* must request *DPoP*-bound *access tokens* from the *Producer Knode*.

To request a *DPoP*-bound *access token*, the *Consumer* includes in the request a *DPoP* proof, sealed with its own private cryptographic material, and provides the corresponding public cryptographic material (hereinafter, proof key).

The *Producer Knode* verifies the *DPoP* proof with the proof key. If it is valid, it issues an *access token* that includes a reference to it, binding the *access token* to it. Thus, the *access token* cannot be used by subjects that do not possess the private cryptographic material associated with the proof key.

To call the *Cross-Border E-Service* with a *DPoP*-bound *access token*, the *Consumer* attaches a *DPoP* proof to every request. The *Producer* must verify the signature of the *DPoP* proof against the proof key to which the *access token* is bound.

The implementation details of the token endpoint for issuing *DPoP*-bound *access tokens*, which the *Producer Knodes* must implement, shall be part of the *Knodia* specification produced by the Federated Consortium, as described in § 5.11 "Considerations on the governance of Knodia".

***Consumers* must ensure the following requirements are met:**

- **They must request a *DPoP*-bound *access token* from the *Producer Knode* corresponding to the *Cross-Border E-Service* of interest and to a specific active *Purpose Statement*.**
- **They must use the *DPoP*-bound *access token* issued by the *Producer Knode* and a *DPoP* proof to request access to the *Producer* for the *Cross-Border E-Service* of interest.**

***Producer Knodes* must ensure the following requirement is met:**

- **They must implement the token endpoint that issues *DPoP*-bound *access tokens* in accordance with the *Knodia* specification and make it available to *Consumers*.**

***Producers* must ensure the following requirement is met: - They must validate the *DPoP*-bound *access token* and the *DPoP* proof sent by the *Consumer* before granting access to their *Cross-Border E-Service*.**

5.8 Knode API for Confederate Organizations

Every *Knode* must allow the *Confederate Organizations* of other *Knodes* to access the functionality offered in its user interface, also through a machine-to-machine API. This allows *Confederate Organizations* to manage entities (e.g., *Cross-Border E-Services*, *Agreement Requests*, *Purpose Statements*) programmatically.

This API can be considered analogous to a *Cross-Border E-Service* produced by the manager of the *Knode*, and which *Confederate Organizations* within *Knodia* can con-

sume. Thus, access to this API is regulated similarly to *Cross-Border E-Services*, except that *Agreement Requests* and *Purpose Statements* are not needed: the agreement between the parties has implicitly occurred during the onboarding of the *Confederate Organization* to *Knodia*. However, *Confederate Organizations* must still create keychains to request *access tokens* for these APIs.

The implementation details of the machine-to-machine API for *Confederate Organizations*, which the *Producer Knodes* must implement, shall be part of the specification of *Knodia* produced by the Federated Consortium, as described in § 5.11 "Considerations on the governance of Knodia".

***Knodes* must ensure the following requirement is met:**

- **They must provide machine-to-machine APIs to the *Confederate Organizations* of *Knodia*.**

5.8.1 Interop Keychains for the Knode API

Interop Keychains are used by *Confederate Organizations* to request *access tokens* for the machine-to-machine API of a *Knode*, hereinafter referred to as the target *Knode*. They are like the *Consumer Keychains* described in § 5.6 "Consumer Keychains", except for these differences:

- They are not associated with any *Purpose Statement*.
- By default, they can only be used to perform read operations.
- To be enabled for create, edit, or delete operations, they require an *Operator* of the *Confederate Organization* to assume responsibility for the operations performed with it. This assumption of responsibility must be made towards all target *Knodes* with which the *Confederate Organization* intends to interact.

An *Operator* who declares responsibility for an *Interop Keychain* assumes administrative responsibility for all operations performed with it. To make this declaration, the *Operator* must:

1. Access the *Interop Keychain* details in the user interface of their *Knode*.
2. Select the target *Knode* they intend to issue the declaration of responsibility towards.
3. Be redirected to the user interface of the target *Knode*.
4. Authenticate via *eIDAS login* and confirm the operation.

The assumption of responsibility towards the target *Knode* therefore works similarly to the confirmation process described in § 5.5.1.1 "Agreement Request – Confirmation by the Consumer Operator".

The target *Knode* that receives the declaration must *Store* the references:

- Of the *Interop Keychain*.
- Of the responsible *Operator*.

After the declaration, the *Keychain* is enabled for create, edit, and delete operations towards the target *Knode*.

***Knodes* must ensure the following requirements are met:**

- **They must make *Interop Keychain* management available to their *Confederate Organizations*.**
- **They must allow *Operators* of their *Confederate Organizations* to issue responsibility declarations for an *Interop Keychain* towards other *Knodes*.**
- **They must allow *Operators* of *Confederate Organizations* of other *Knodes* to confirm the responsibility declaration for their *Interop Keychain*.**

5.8.2 Interop access tokens

Using an *Interop Keychain*, a *Confederate Organization* can request an *interop access token* to the target *Knode*. To do this, it must send a request with a client assertion, as described in § 5.7 “Issuance of access tokens for Cross-Border E-Services”, with the following differences:

- The audience must be one of those declared in the *Knode*'s API specification.
- No *Purpose Statement* identifier is included.
- It must include the identifier of the *Knode* of the requester *Confederate Organization*, on which the *Interop Keychain* is stored. This allows the target *Knode* to retrieve the *Keychain* data using the *Knodia API* to verify the client assertion.

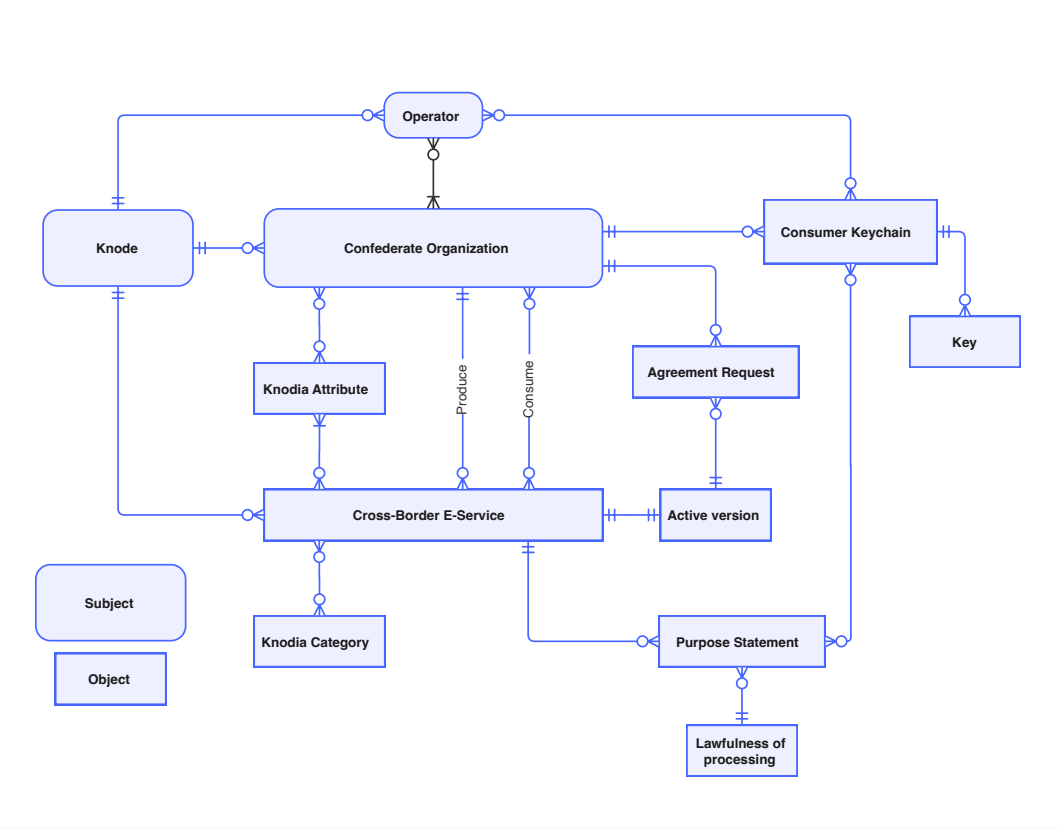
***Knodes* must ensure the following requirements are met:**

- **They must make the public cryptographic material deposited in *Interop Keychains* available to other *Knodes* through the *Knodia API*.**
- **They must retrieve the public cryptographic material of *Interop Keychains* from other *Knodes* to verify *client assertions*.**
- **They must issue *interop access tokens* that allow create, edit, or delete operations to *Confederate Organizations* of *Knodia* only if the declaration of responsibility was made by an *Operator* of the *Organization*; otherwise, only allow read operations.**

5.9 Lifecycle of entities

This section describes the lifecycle of the *Cross-Border E-Service*, *Agreement Request*, and *Purpose Statement* entities.

To help the reader consider these entities in their context, the following diagram illustrates them, and others cited heretofore, with their relationships expressed in crow’s foot notation.



5.9.1 Lifecycle of Cross-Border E-Services

A *Cross-Border E-Service* can have one or more versions. *E-Service* versioning allows the *Producer* to update the description of the provided functionality (for example, by uploading an updated OpenAPI specification).

This concept was not mentioned so far to keep the presentation simpler.

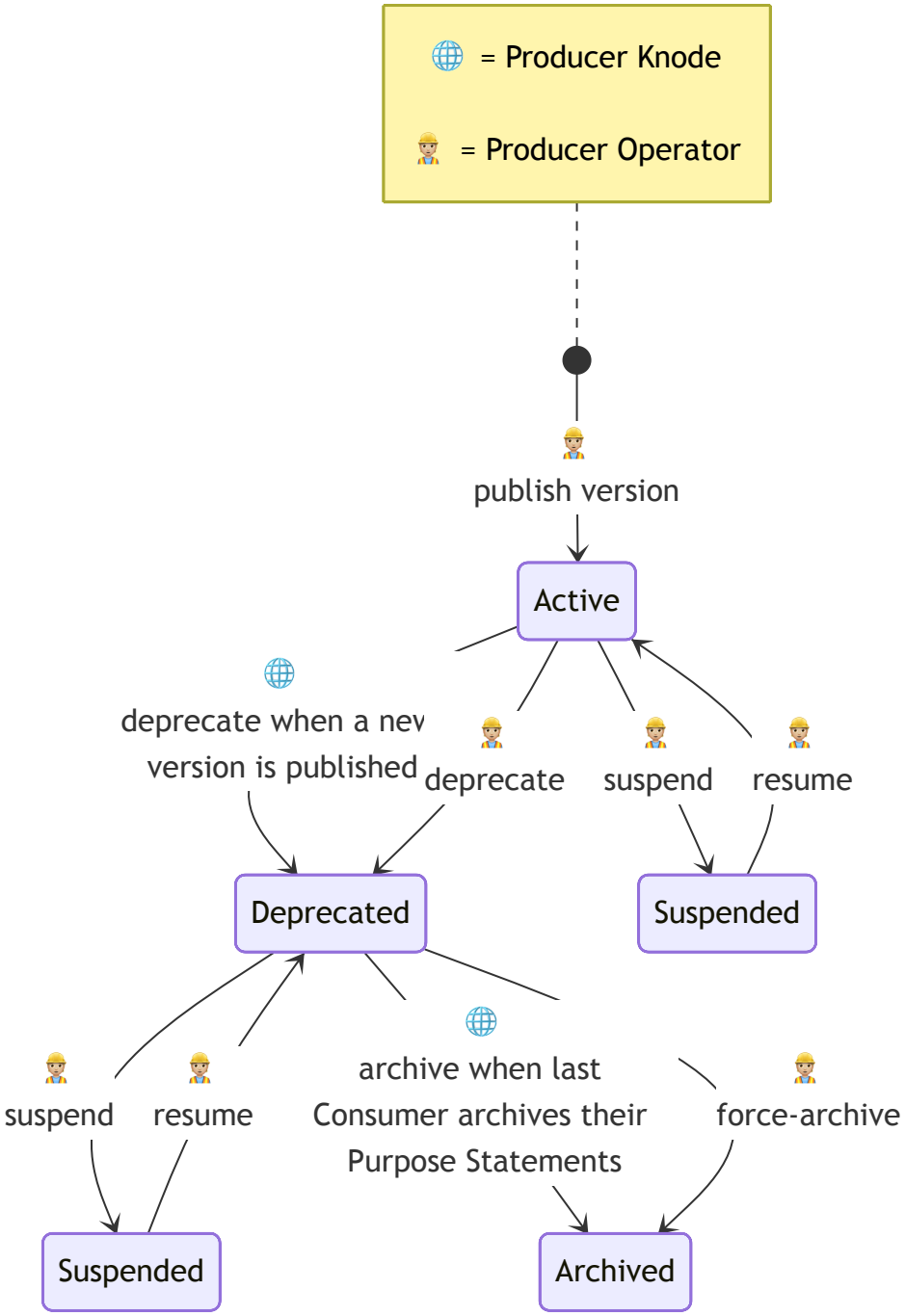
The first version of the *Cross-Border E-Service* is created by the *Producer* at the same time as the *Cross-Border E-Service* itself. Afterwards, the *Producer* can create and publish an updated version. This automatically deprecates the existing version.

Creating a new version does not prevent *Consumers* from continuing to consume the previous, now deprecated, versions. However, *Consumers* must be notified that a new version has been published and the one they are consuming is deprecated. The notification should prompt *Consumers* to upgrade to consume the new version. *Agreement Requests* are themselves associated with a specific version, not with the *Cross-Border E-Service*.

The following diagram represents the states and lifecycle of each *E-Service* version. State transitions in the diagram are labelled with an icon to identify the actors that can perform that action.

Relevant states for *Cross-Border E-Service* versions are:

- **Active:** The *Cross-Border E-Service* version has been published in the catalogue and is available for use.
- **Suspended:** The *Producer* has temporarily suspended operation of the *Cross-Border E-Service* – e.g., due to technical or administrative problems – but can reactivate it later. This suspends issuance of *access tokens*.
- **Deprecated:** The *Producer* has marked the version as deprecated or has created a new version for the *Cross-Border E-Service*, noting that this version will be disabled in the future. New *Agreement Requests* for that version are not accepted. A deprecated version can still be used; therefore, it too can be temporarily suspended if needed.
- **Archived:** The version is no longer operating and will not be reactivated. The *Producer* can manually archive a deprecated version (respecting advance notification to *Consumers* and other conditions the *Knode* can impose). Archiving also occurs automatically when the deprecated version is no longer consumed by any *Consumer*.

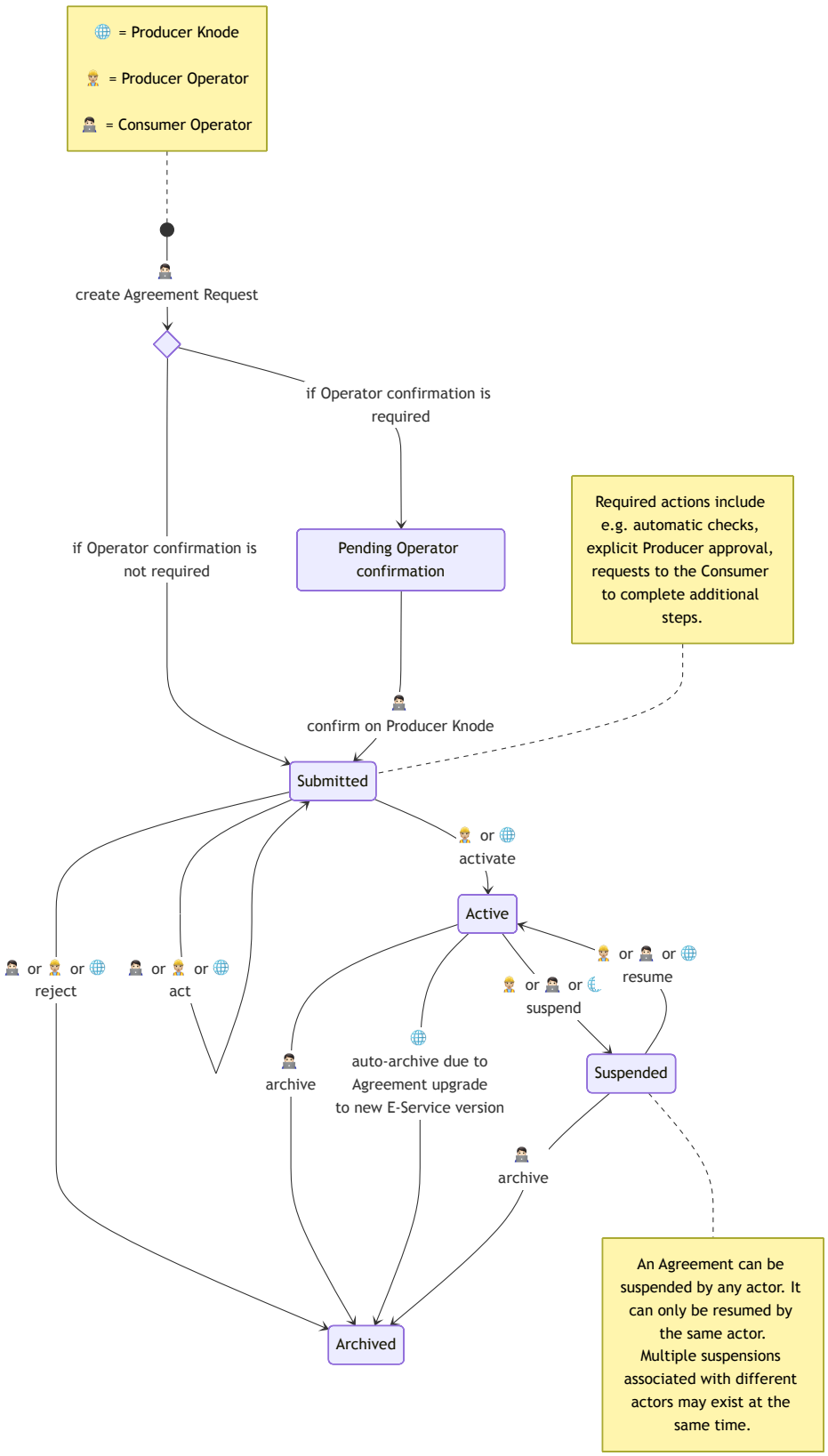


5.9.2 Lifecycle of Agreement Requests

The following diagram illustrates the lifecycle of an *Agreement Request*, starting when the *Consumer* requests its creation through its *Consumer Knode*. The diagram uses choice nodes to indicate that confirmation via *eIDAS login* is optional.

The states are:

- **Pending Operator confirmation:** The *Agreement Request* is created by the *Producer Knode* in this state if the *Producer* requested confirmation from a *Consumer Operator* via *eIDAS login* on the *Producer Knode* for that *Cross-Border E-Service*.
- **Submitted:** The *Agreement Request* has been created but is not active yet. Depending on the policy of the *Producer Knode*, it could be activated or rejected automatically, or it could require manual approval. The *Consumer* could also be asked (automatically or after a manual action by the *Producer*) to complete further steps. The *Agreement Request* leaves this state if it is activated (by the *Producer* or automatically by the *Producer Knode*) or archived (because it is rejected by the *Producer*, automatically rejected by the *Producer Knode*, or deleted by the *Consumer*).
- **Active:** The *Agreement Request* has been approved and is active. The *Consumer* can request *access tokens* to be issued for the corresponding *E-Service*.
- **Suspended:** The *Agreement Request* has been temporarily suspended, e.g., due to technical or administrative problems. The *Consumer* cannot request *access tokens* for the corresponding *E-Service*. The *Agreement Request* can be suspended by the *Producer*, by the *Consumer*, or automatically by the *Producer Knode* (for example, if the *Consumer* no longer has one of the *Knodia Attributes* in the *consumption requirements*). Multiple actors can suspend the *Agreement Request* contemporaneously. The *Agreement Request* is then reactivated only if all actors who had suspended it reactivate it.
- **Archived:** The *Agreement Request* has been archived and is no longer valid. The *Consumer* can manually archive an *Agreement Request*. An *Agreement Request* is also archived if it is rejected or if intervening conditions prejudice its existence.

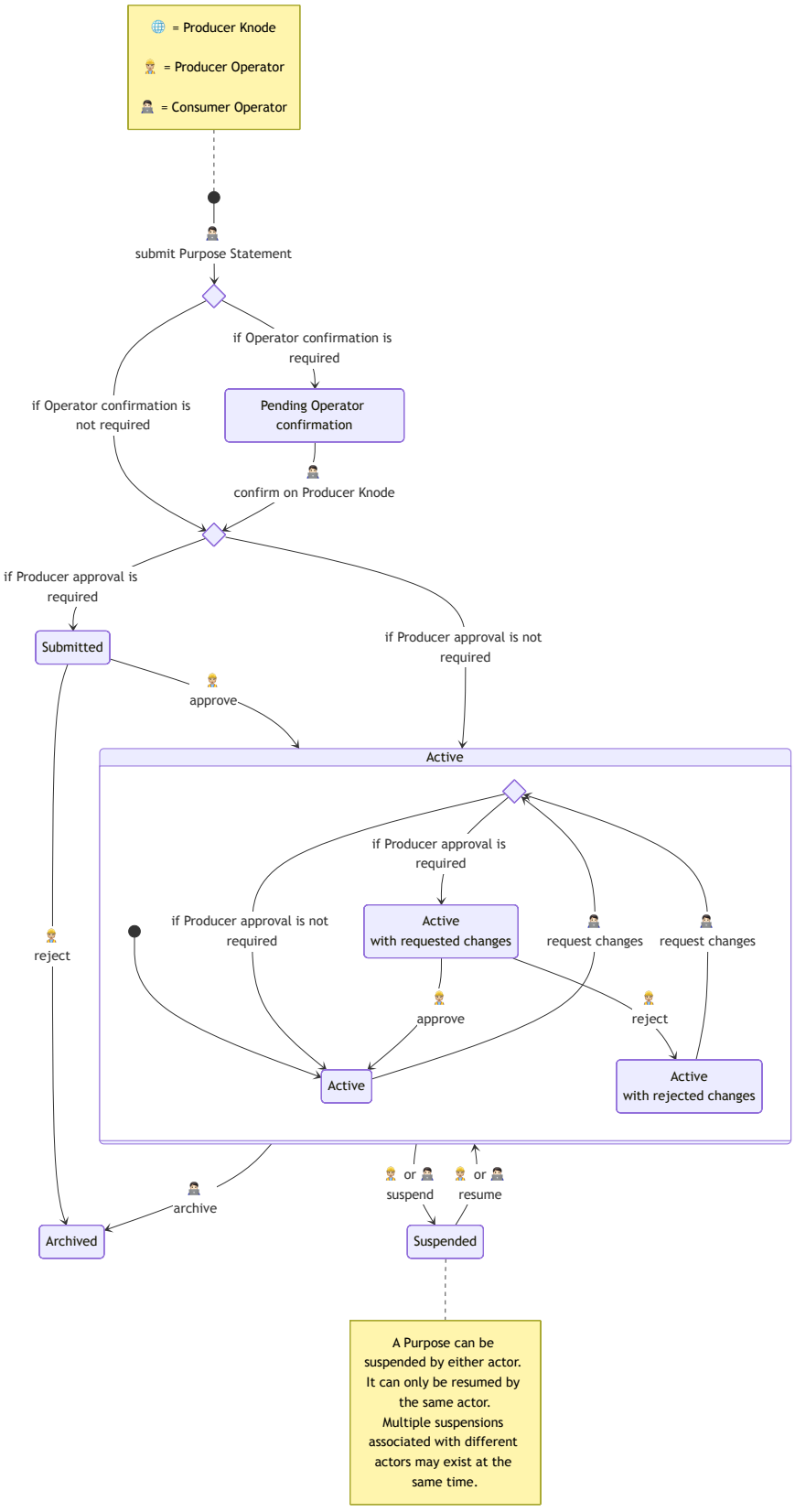

🌐 = Producer Knode
🧑‍💼 = Producer Operator
👨‍💻 = Consumer Operator
👨‍💻
create Agreement Request
if Operator confirmation is required
if Operator confirmation is not required
Pending Operator confirmation
Required actions include e.g. automatic checks, explicit Producer approval, requests to the Consumer to complete additional steps.
👨‍💻
confirm on Producer Knode
Submitted
🧑‍💼 or 🌐
activate
Active
👨‍💻 or 🧑‍💼 or 🌐
reject
👨‍💻 or 🧑‍💼 or 🌐
act
🧑‍💼 or 👨‍💻 or 🌐
resume
🧑‍💼 or 👨‍💻 or 🌐
suspend
Suspended
👨‍💻
archive
🌐
auto-archive due to Agreement upgrade to new E-Service version
👨‍💻
archive
Archived
An Agreement can be suspended by any actor. It can only be resumed by the same actor. Multiple suspensions associated with different actors may exist at the same time.

5.9.3 Lifecycle of Purpose Statements

The following diagram illustrates the lifecycle of a *Purpose Statement* created by a *Consumer* to access a *Provide-Data Cross-Border E-Service*. In the diagram, choice nodes represent optional steps, and a composite state represents the possible sub-states for an active *Purpose Statement*.

The states are:

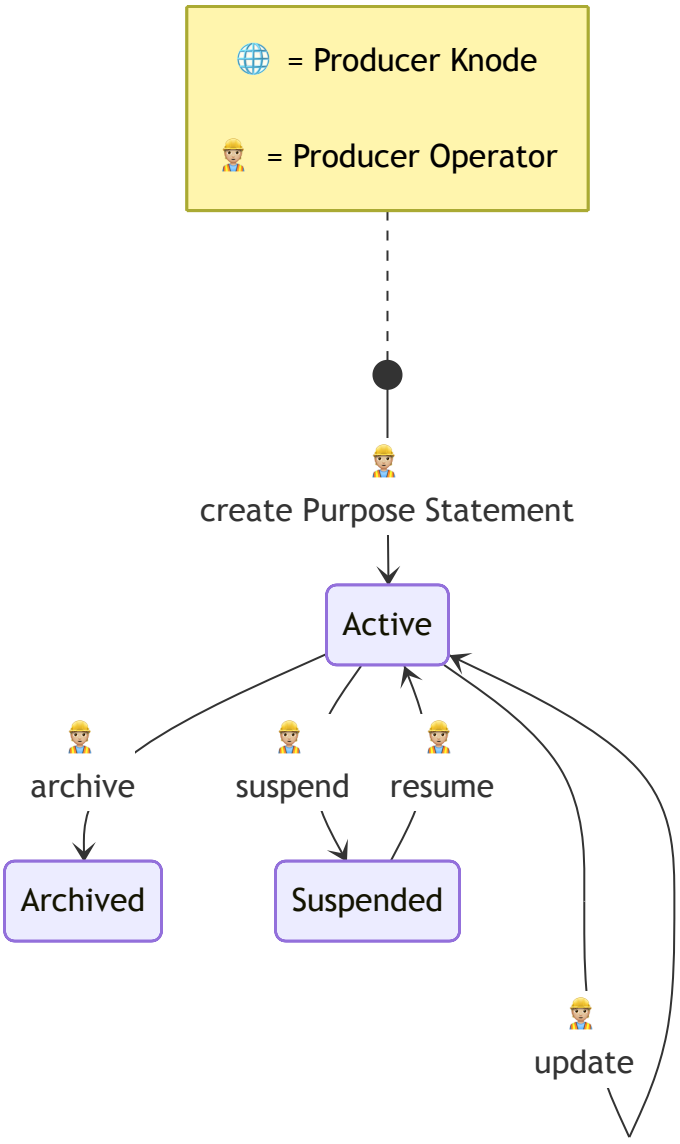
- **Pending Operator confirmation:** The *Purpose Statement* is created by the *Producer Knode* in this state if the *Producer* requested confirmation from a *Consumer Operator* via *eIDAS login* on the *Producer Knode* for that *Cross-Border E-Service*
- **Submitted:** The *Purpose Statement* has been created, but the *Producer* must approve it. The *Producer* can approve it or reject it. *Producer* approval may not be necessary, depending on the policies of the *Producer Knode*.
- **Active:** The *Purpose Statement* has been approved and is active. The *Consumer* can request *access tokens* for the corresponding *E-Service*. This state includes two distinct sub-states:
  - **Active, with requested changes:** The *Consumer* has requested to update the *Purpose Statement*. The *Purpose Statement* remains in its current state until the changes are applied, in accordance with the policies of the *Producer Knode*.
    - Note: This state is necessary to let the *Consumer* update an active *Purpose Statement*, for example, to change the expected load (maximum number of requests per unit of time), without losing access to the *Cross-Border E-Service* while the approval is pending. The *Consumer* could, alternatively, create a new *Purpose Statement*, with the new load, and keep the previous one active until the new one is activated, and then archive it. However, if the *Producer Knode* limits the creation of new *Purpose Statements* based on the *Cross-Border E-Services* quotas, this might not be possible: the *Consumer* might not be able to create a new *Purpose Statement* until it has archived the existing one. Modelling the change request explicitly avoids this issue.
  - **Active, with rejected changes:** The changes requested by the *Consumer* have been rejected. The *Purpose Statement* remains unchanged. The *Consumer* may request new changes.
- **Suspended:** The *Purpose Statement* has been temporarily suspended, e.g., due to technical or administrative problems. The *Consumer* cannot request *access tokens* for the corresponding *E-Service*. The *Purpose Statement* can be suspended by the *Producer*, by the *Consumer*, or by both. It is again active only if all actors who had suspended it reactivate it.
- **Archived:** The *Purpose Statement* has been archived and is no longer valid. The *Consumer* can manually archive a *Purpose Statement*. A *Purpose Statement* is also archived if the *Producer* refuses to activate it.


= Producer Knode
= Producer Operator
= Consumer Operator
submit Purpose Statement
if Operator confirmation is required
if Operator confirmation is not required
Pending Operator confirmation
confirm on Producer Knode
if Producer approval is required
if Producer approval is not required
Submitted
approve
reject
Active
if Producer approval is required
if Producer approval is not required
Active with requested changes
request changes
request changes
approve
reject
Active
Active with rejected changes
archive
or suspend
or resume
Archived
Suspended
A Purpose can be suspended by either actor. It can only be resumed by the same actor. Multiple suspensions associated with different actors may exist at the same time.

The following diagram illustrates the lifecycle of a *Purpose Statement* created by a *Producer* for one of its *Receive-Data E-Services*.

The states are:

- **Active:** The *Purpose Statement* has been created and is active. In this state, the *Producer* can also update the *Purpose Statement*.
- **Suspended:** The *Purpose Statement* was temporarily suspended, e.g., due to technical or administrative problems. *Consumers* cannot request *access tokens* for the corresponding *E-Service*.
- **Archived:** The *Purpose Statement* has been archived and is no longer valid.



5.10 Additional functionality provided by Knodes

This section describes additional functionality that *Knodes* may provide to *Confederate Organizations* in *Knodia* to simplify cross-border interoperability between them. The experience with the *PDND* in Italy has already demonstrated its value to organizations.

5.10.1 Asynchronous communication

Consumption, as described so far, occurs synchronously: the *Cross-Border E-Service* responds to the *Consumer*'s request with the requested data. A *Knode* must also provide an alternative asynchronous mode that *Producers* can use to respond.

A *Producer* that intends to use the asynchronous mode for a *Cross-Border E-Service* must declare the characteristics of the callback endpoint that the *Consumer* must implement to receive the data.

When calling the *Cross-Border E-Service*, the *Consumer* specifies the callback endpoint. When the *Producer* completes processing the request and is ready to return the resources, it calls the callback endpoint specified by the *Consumer*.

The *Knodia Consortium*, referred to in § 5.11 "Considerations on the governance of Knodia", capitalizing on the effects of the proposed experimentation, defines in detail how to implement this functionality.

5.10.2 Distribution of data change signals (Signal Hub)

Beyond the usual model of consumption (i.e., a *Consumer* calls the *Cross-Border E-Services* offered by *Producers*), the *Knode* may also provide a signal distribution system that lets *Consumers* detect when a change occurs in the data provided by a *Cross-Border E-Service* (which the *Consumer* is authorized to consume), referring to entities the *Consumer* is interested in.

This functionality is intended to allow *Consumers* to react promptly to updates to information on subjects for whom the *Consumer* has outstanding processing operations, while avoiding excessive load on *Producers* (which would be imposed by *Consumers* repeatedly fetching the data to monitor it for changes). Moreover, this standardizes, throughout *Knodia*, a single model for distributing data changes.

To support this, the *Knode* must implement a service, here referred to as the *Signal Hub*. The *Signal Hub* allows *Producers* of that *Knode* to deposit signals related to data changes for a *Cross-Border E-Service* after enabling the *Signal Hub* for that service. It allows any *Consumer* throughout *Knodia* to retrieve the signals they are interested in. To retrieve signals, the *Consumer* needs an active *Agreement Request* and at least one active *Purpose Statement* for the *E-Service*.

The *Knodia Consortium*, referred to in § 5.11 "Considerations on the governance of Knodia", capitalizing on the effects of the proposed experimentation, defines in detail how to implement this functionality.

The remainder of this section reports considerations on this functionality based on the experience with the *PDND* in Italy.

5.10.2.1 Signals and pseudonymization

A signal is an object that notifies of a data change. It identifies the entity whose data changed. Entities are identified pseudonymously, using a hashing algorithm. This allows the *Consumer* to reconcile them by comparing the entity identifiers the *Consumer* already knows with their pseudonymous representation included in the signals.

To make pseudonymization more secure, hashing with a seed[1] is used. The *Producer* must expose in its *E-Service* the reference to the hashing algorithm and the seed it currently uses.

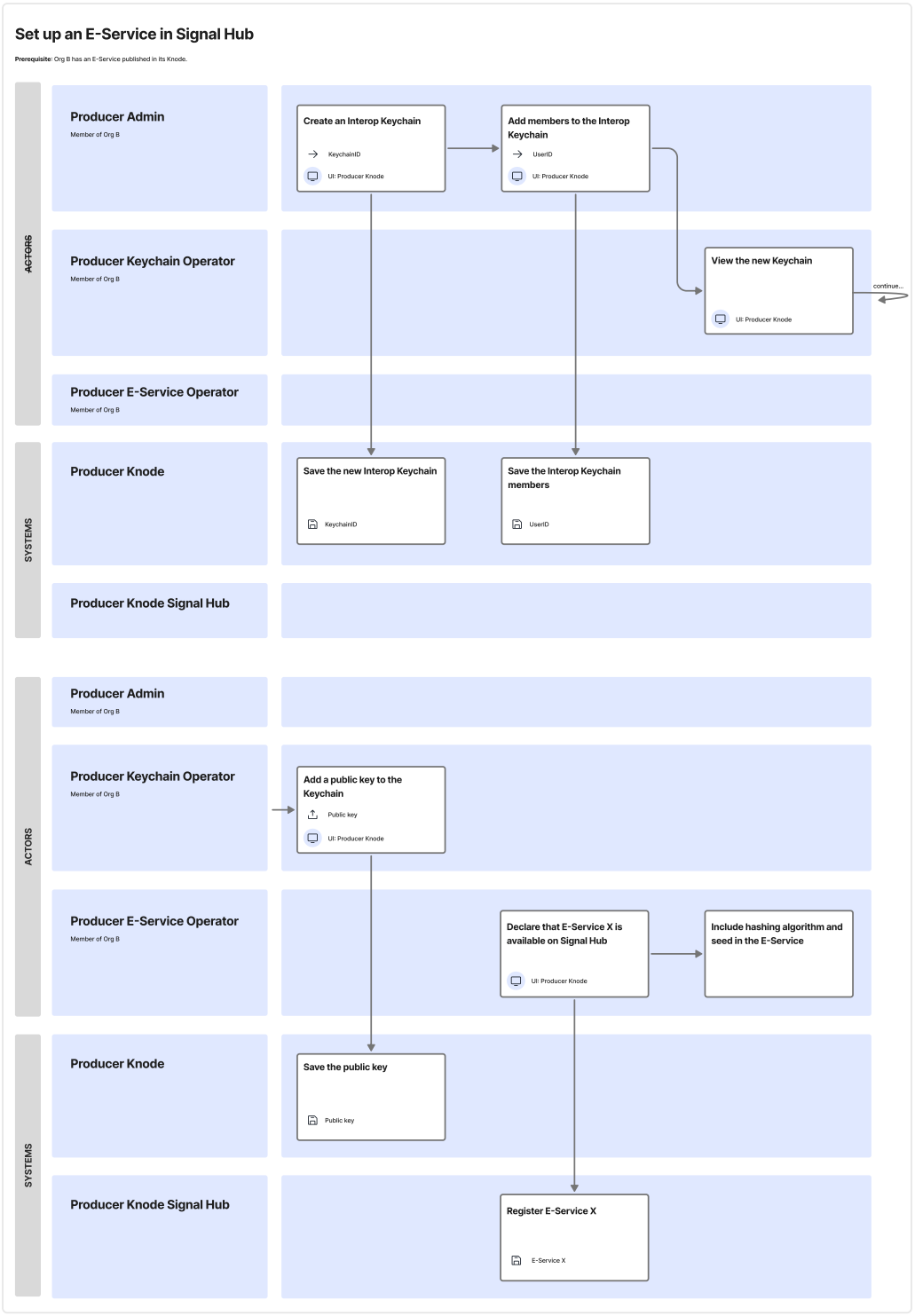
In addition to signals related to entity lifecycle changes, the *Producer* must also deposit signals to assist with signal processing itself: specifically, signals that notify of changes in the hashing algorithm or the seed.

5.10.2.2 Signal deposit, retrieval, and processing flow

A *Producer* that intends to make signals available for data changes for a *Cross-Border E-Service* must enable the *Signal Hub* for this *E-Service*. The *Producer* must also create an *Interop Keychain* to request *access tokens* to access the *Signal Hub* (see § 5.8.1 “Interop Keychains for the Knode API”).

The following service blueprint illustrates the steps to make signals available for a *Cross-Border E-Service* (exemplifying also a possible subdivision of roles for *Organization Operators*).

[1] The Italian implementation of the *Signal Hub* for the *PDND* has followed the report “Pseudonymisation techniques and best practices” of the ENISA, available at the URL https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.



When a data change occurs, the *Producer* requests an *interop access token* to access the *Signal Hub* (using the normal token request process) and deposits the signal by calling the *Signal Hub* API.

The following service blueprint illustrates the signal deposit process.

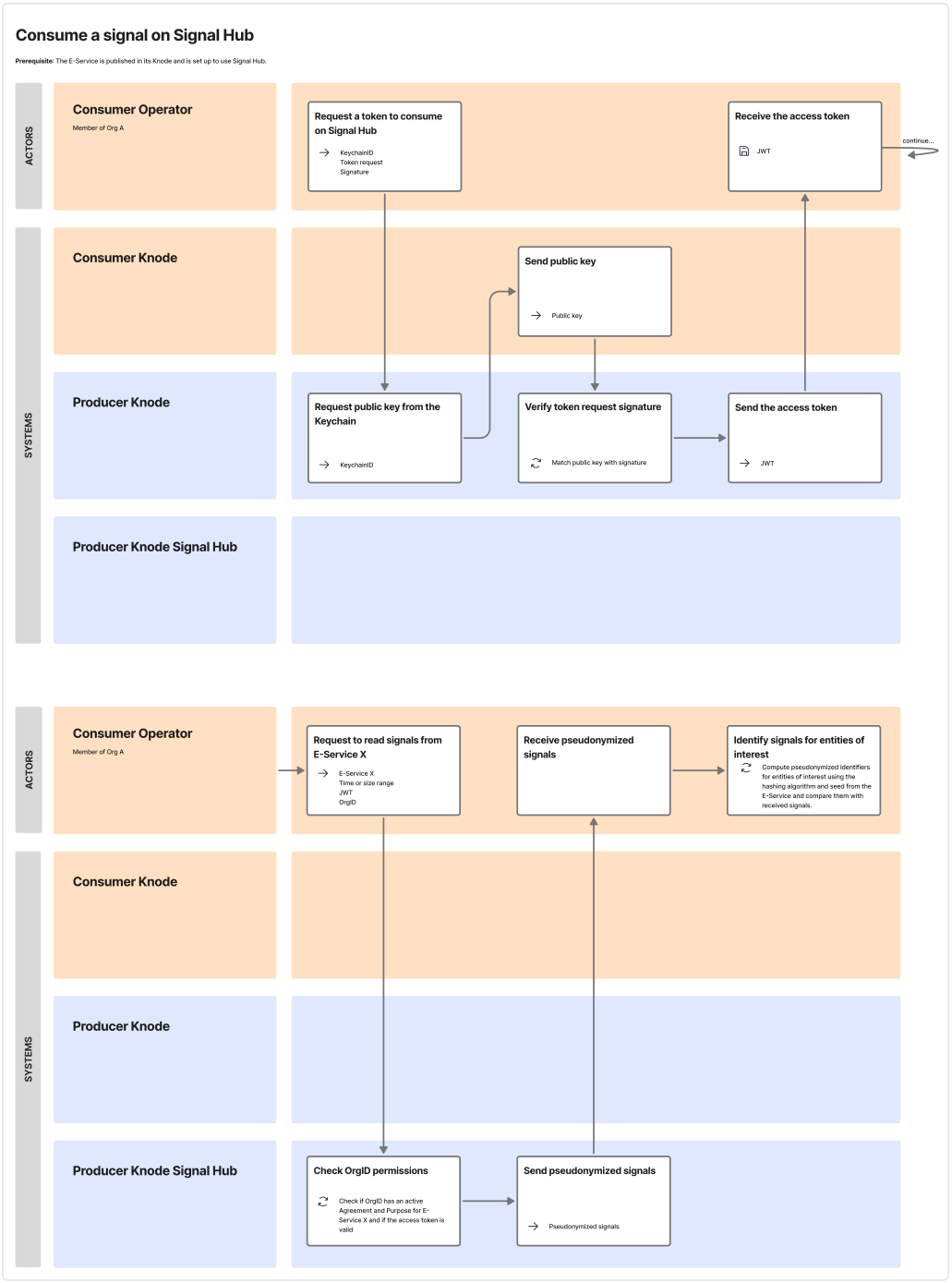
The *Signal Hub* persists the signal for an interval defined in the policy of *Knodia* and automatically deletes it after that time.

A *Consumer* interested in data changes for the *Producer*'s *E-Service* must, like the *Producer*, create an *Interop Keychain* to request tokens to access the *Signal Hub* service of the *Producer Knode*. Using this token, the *Consumer* periodically accesses (by polling) the *Signal Hub* to retrieve all signals deposited for that *E-Service*.

A signal does not include the data itself: it is only a notification that the data changed. Hence, the *Consumer* must process the signals to determine which refer to entities of interest. Then, it may retrieve the new state of those entities by calling the *Producer*'s *E-Service* directly.

To process the signals, the *Consumer* must compute the pseudonymous identifiers of all entities of interest (using the hashing algorithm and seed communicated by the *Producer*) and compare them with those in the signals.

The following service blueprint illustrates the signal retrieval process.



5.10.3 E-Service Templates

An *E-Service Template* standardizes the creation of *Cross-Border E-Services* for recurring use cases. If many *Producers* need to provide *Cross-Border E-Services* following the same specification, one *Producer* may create an *E-Service Template* and publish it on its *Knode*. The template is then available to other *Confederate Organizations* that

need to produce similar *Cross-Border E-Services*.

Every *Producer* can view the *E-Service Templates* available on both its own and other *Knodes*. It can create a *Cross-Border E-Service* by instantiating one such template. The *E-Service* so created inherits all predefined fields from its template, including the application programming interface (API) specification. However, the template creator can specify fields that the *Producer* can override when instantiating the template.

E-Service Templates, like *Cross-Border E-Services*, can have multiple versions. When a new version is created, the previous versions are automatically deprecated. New instances can only be created from the latest version. However, *E-Services* instantiated from an older version may still exist. The *Knode* must notify (possibly via other *Knodes*) the *Producers* that have instantiated an *E-Service Template* when a new version of the template is published, and (if it's the case) that the version currently in use will no longer be available after a given date.

The *Knodia Consortium*, referred to in § 5.11 "Considerations on the governance of Knodia", capitalizing on the effects of the proposed experimentation, defines in detail how to implement this functionality.

5.10.4 Purpose Statement Templates

Knodes may also provide *Purpose Statement Templates* that *Confederate Organizations* can use to obtain a pre-filled version of the *Purpose Statement*, including any additional information requested from *Consumers* in accordance with the national regulatory framework.

A *Consumer* with an active *Agreement Request* for a *Cross-Border E-Service* can view the *E-Service*'s *Purpose Statement* Templates, if there are any, and choose whether to use them when creating a *Purpose Statement*.

Using a *Purpose Statement* Template does not exempt the *Consumer* from responsibility for the *Purpose Statement* it creates.

The *Knodia Consortium*, referred to in § 5.11 "Considerations on the governance of Knodia", capitalizing on the effects of the proposed experimentation, defines in detail how to implement this functionality.

5.10.5 Producer Keychains

A *Knode* may allow *Producers* to create one or more *Producer Keychains* to associate with their *Cross-Border E-Services*. These objects are equivalent to the *Consumer Keychains* described in § 5.6 "Consumer Keychains".

Using the public cryptographic material deposited in the *Producer Keychain*, *Producers* can electronically seal the responses their *Cross-Border E-Services* send. This assures *Consumers* within *Knodia* non-repudiation for these responses.

If the *Producer* uses this functionality, its *Knode* must make the contents of the *Producer*

Keychain available via the *Knode* API. This allows *Consumers* to retrieve the public cryptographic material and verify the seal of the *E-Service*'s responses.

5.11 Considerations on the governance of Knodia

As mentioned at the beginning, a *Knodia Consortium* – including the Managers of the *Knodes* – will need to exist. This *Consortium* will define and update the technical elements needed for *Knodia*, capitalizing on the effects of the proposed experimentation.

The main task of this *Consortium* is to define the *Knodia API* to be implemented by *Knodes* and to manage the semantic objects used by *Knodes*.

The *Knodia Consortium* will be responsible for defining and evolving the shared artifacts necessary to enable *cross-border interactions*. Specifically, these include:

- The controlled vocabularies of *Knodia Attributes* and *Cross-Border E-Service Knodia Categories* (as defined in the corresponding sections).
- The specification of the *Knodia API*, that every *Knode* must provide to other *Knodes* to retrieve data and events for the various resources (this should be based on the needs identified in § 5.11.1 “Distribution of knowledge between Knodes”).
- The set of events that *Knodes* need to track for each resource and to publish (using dedicated endpoints of the *Knodia API*) so other *Knodes* can react to them.
- The specification of the *Knode* API that every *Knode* must provide to *Confederate Organizations* to retrieve and manage resources programmatically.
- The definition of the format of the *Purpose Statement* forms exchanged between *Knodes*.
- The details of the additional functionality proposed in § 5.10 “Additional functionality provided by Knodes”.
- Any vocabulary, ontology, specification, or data schema for which the need emerges during the prototyping and evolution of *Knodia*.

5.11.1 Distribution of knowledge between Knodes

To implement the functionality described in this proposal, *Knodes* need to communicate with each other. Two modes of communication are envisioned:

1. Queries and commands that a *Knode* sends to another – synchronously – while processing a request from an *Operator* or, in general, to perform the described flows.
2. Propagation of events for state changes of entities (*Confederate Organizations* and *Knodia Attributes* associated with them, *Cross-Border E-Services*, *Agreement Requests*, *Purpose Statements*, etc.) from the *Knode* where the change occurs to other interested *Knodes*.

Note that, in both cases, the data exchanged between *Knodes* does not contain personal data of natural persons.

The first mode of communication occurs, for example, when searching for *Cross-Border E-Services* offered in another *Knode* or when creating an *Agreement Request*. These communications can be classified as either queries (read operations that do not change the state of the *Knodes*) or commands (by which, e.g., a *Knode* requests that another Knode create an entity, such as an *Agreement Request* or *Purpose Statement*).

The second mode is used to forward relevant events between *Knodes*, ensuring their states are consistent. These events include, for example, the revocation of a *Knodia Attribute* of a *Confederate Organization* or the suspension of an *Agreement Request* by the *E-Service Producer*. Cases where the event is generated by a *Knode*, but it is helpful to propagate it to other *Knodes* so they can update the state of other entities and/or notify the *Organizations* concerned.

5.11.1.1 Means of communication

Both modes of communication are implemented as HTTP APIs, using JSON for request and response bodies. This API was heretofore referred to as the *Knodia API*. Every *Knode* must implement the endpoints of this API in accordance with an OpenAPI specification to be defined by the *Knodia Consortium*, capitalizing on the effects of the proposed experimentation.

Synchronous queries and commands will therefore be implemented as HTTP requests (with methods GET, POST, or other as appropriate) from a *Knode* to another.

For event propagation, every *Knode* must provide endpoints that allow other *Knodes* to retrieve events generated by that *Knode*. Propagation is therefore by *pull*: the *Knode* that is interested in the events must periodically make a request (*polling*).

We consider the pull strategy preferable to a push one (e.g., using webhooks) so the *Knode* does not have to manage fan-out (e.g., for each event, call the webhooks of all other *Knodes*), nor retries in case the target *Knode* is temporarily unreachable (which is an occurrence the source *Knode* cannot control). A pull strategy makes the source *Knode* responsible only for reliably providing its endpoints.

The proposed approach, based on polling, could be replaced by a *Knode* exposing a message broker to which other *Knodes* can connect as consumers. This option could be more efficient in terms of latency and throughput. However, mandating that every *Knode* include a message broker imposes stricter technical constraints on implementers. If a single message broker is standardized throughout *Knodia* (e.g., Kafka), every *Knode* implementer is forced to adopt it. If several are supported (e.g., a *Knode* could use Kafka and another an AMQP-compliant broker), implementers must support several protocols to consume events from multiple *Knodes*. A pull-based HTTP API leaves implementers greater technological autonomy while keeping a standard interface. *Knodes* can still, at their discretion, use message brokers or queues internally.

To guarantee event retrieval is efficient, the dedicated endpoints must include filters to select the events to retrieve. For instance, each *Knode* is interested only in retrieving events related to *Agreement Requests* involving their *Organizations* and other entities

associated with that *Agreement Request*.

5.11.2 Configuration of the federation of Knodes

In this proposal, we assume that, for each *Knode*, the other *Knodes* are trusted subjects with a secure communication channel. We assume this channel will be implemented using mutual TLS.

The interactions between *Knodes* described in this proposal implicitly assume that a secure channel exists. Therefore, they do not include explicitly the transmission of any additional cryptographic material between them.

In the foreseen use cases, a limited number of *Knodes* will exist, and they will not change frequently. For example, there could be one *Knode* per Member State of the European Union and one for the European Union institutions. Therefore, even a relatively burdensome process for establishing secure communication between two *Knodes* seems acceptable (for instance, one that involves certificate exchange), and we do not envision a need for protocols for automatic discovery of new *Knodes*.

The *Knodia Consortium*, capitalizing on the effects of the proposed experimentation, defines the process for new *Knodes* to join *Knodia* and the means to exchange the necessary elements to establish trust between the *Knodes*.

Chapter 6

Annex

6.1 Glossary

Term	Acronym	Definition
Agreement Request		The request by a *Confederate Organization* to use a *Cross-Border E-Service*.
Application Programming Interface	API	An interface that allows different software to communicate with each other, exchanging data and functionality.
Confederate Organization		A public or private organization which has completed the identification process (onboarding) on the *Knode* to which it belongs based on territorial, administrative, or organizational competence.
Consumer Knode		The *Consumer*'s *Knode*.
Consumer		A *Confederate Organization* that uses a *Cross-Border E-Service*.
Cross-Border E-Service		An *E-Service* enabled by the *Producer* for *cross-border interactions*.
Cross-border interaction		A digital interaction performed by subjects belonging to distinct *Knodia Domains*, performed to ensure the exchange of data or integration of services.
Electronic Archiving		As defined in the *eIDAS Regulation*.
Electronic seals		As defined in the *eIDAS Regulation*.
European Interoperability Framework	*EIF*	As defined in the *Interoperable Europe Act*.
Innovation measures		As defined in the *Interoperable Europe Act*.
Interoperability assessment		As defined in the *Interoperable Europe Act*.
Interoperability Node	*Knode*	The component of *Knodia* to enable *cross-border interactions*.
Interoperability regulatory sandbox		A controlled environment established by a European Union entity or a public body for the development, training, testing, and validation regarding innovative interoperability solutions, where appropriate in real-world conditions, supporting the cross-border interoperability of trans-European digital public services for a limited period of time under regulatory supervision.
Interoperability solutions		As defined in the *Interoperable Europe Act*.

Term	Acronym	Definition
Interoperable Europe Agenda		As defined in the *Interoperable Europe Act*.
Interoperable Europe Board		As defined in the *Interoperable Europe Act*.
Interoperable Europe Community		As defined in the *Interoperable Europe Act*.
Interoperable Europe portal		As defined in the *Interoperable Europe Act*.
Knodia API		The machine-to-machine APIs implemented and used by the *Knodes* to engage in the communication protocols of *Knodia*.
Knodia Attribute		The attributes defined in *Knodia* that are associated with *Confederate Organizations* and used to grant the right to make requests for access to *Cross-Border E-Services*.
Knodia Category		The categories defined in *Knodia* that are used by *Confederate Organizations* to classify their *Cross-Border E-Services* in relation to the nature of the data and services they provide.
Knodia Domain		A set of subjects that have defined and shared common rules, based on mutual trust, to proceed with the sharing of data and services among themselves using digital tools.
Lawfulness of processing		As defined in the *GDPR*.
Modello di interoperabilità	*ModI*	The interoperability model adopted by Italian public administrations.
Monitoring and evaluation		As defined in the *Interoperable Europe Act*.
National competent authorities and single points of contact		As defined in the *Interoperable Europe Act*.
Operator		A natural person associated with a *Confederate Organization* who uses the functionalities made available by the *Knodes*.
Peer review		As defined in the *Interoperable Europe Act*.
Piattaforma Digitale Nazionale Dati	*PDND*	The platform provided for in the *ModI* to authenticate and authorize access to *Cross-Border E-Services*.
Policy implementation support projects		As defined in the *Interoperable Europe Act*.
Porta di Dominio	*PdD*	The component provided for in the *SPCoop* instantiated by individual public administrations to enable machine-to-machine interaction.
Producer Knode		The *Producer*'s *Knode*.
Producer		A *Confederate Organization* that makes *Cross-Border E-Services* available.
Provide-Data		The method of sending data from *Producer* to *Consumer* via a *Cross-Border E-Service*. In this mode, the *Confederate Organization* acquiring new data from the transactions performed is the *Consumer*.
Purpose Statement		The statement made by a *Consumer* to explicitly state the lawfulness of processing under the *GDPR*.
Purpose		The reference to a *Purpose Statement* made by a *Consumer*.
Receive-Data		The method of sending data from *Consumer* to *Producer* via a *Cross-Border E-Service*. In this mode, the *Confederate Organization* acquiring new data from the transactions performed is the *Producer*.
Servizi di Interoperabilità, Cooperazione ed Accesso	*SICA*	The system that implements and makes available the infrastructural services of *SPCoop*.

Term	Acronym	Definition
Signal Hub		The digital tool provided by the *Knodes* to the *Confederate Organizations* of *Knodia* to distribute data changes of interest to *Confederate Organizations*.
Sistema pubblico di cooperazione	*SPCoop*	The application cooperation system adopted by Italian public administrations.
Storing		The digital recording performed by an IT system to secure the information necessary for its operations.
Trans-European digital public service		As defined in the *Interoperable Europe Act*.

6.2 Reading service blueprints

Throughout this proposal, service blueprints illustrate the activities and interactions among entities in *Knodia*. While the blueprint is intended as an intuitive representation, for clarity, the following notes describe the conventions used.

- Each blueprint is organized into horizontal rows (often called *swimlanes*), which separate the entities involved in the process. These entities can be human *actors* (the *Operators* of *Confederate Organizations*) or *systems*. *Knodes* are the systems represented in most blueprints, usually without subdividing them into their internal components.
- Each box within the rows represents an action performed by the corresponding entity. It also indicates:
  - For actions by actors, which user interface is used by the actor (to distinguish actions made on the actor's own *Knode* or on other *Knodes*).
  - The data sent to other entities as a result of the action (right arrow icon).
  - The data stored by the system as a result of the action (save icon).
  - The processing of data executed by the system (circle arrows icon).
- The flow is read by following the arrows, where horizontal arrows represent a sequence of actions performed by the same subject, while arrows crossing into a different row represent an interaction.
- Dashed boxes and arrows indicate optional parts of the flow.

STAKEHOLDERS

Dipartimento per la trasformazione digitale

PagoPA S.p.A.

Get in touch — info@knodia.org