GT de Tecnologías Futuras de AMETIC - Webinar

ESPACIOS DE DATOS COMPARTIDOS: RETOS DE SEGURIDAD

Alberto Berreteaga – TECNALIA – IDS Competence Centre Coordinator
alberto.berreteaga@tecnalia.com

26 de enero de 2024
AMETIC - TECNALIA

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Alberto Berreteaga

IDS Competence Centre Coordinator

Fundación TECNALIA Research & Innovation

Unidad DIGITAL – Core
Grupo Ciberseguridad
IDS Competence Centre

alberto.berreteaga@tecnalia.com
@AlbertoTecnalia

dataspaces@tecnalia.com

tecnalia

MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Trabajando en los Espacios de Datos

Entidades, organizaciones e iniciativas

IDSA – International Data Spaces Association https://internationaldataspaces.org

Gaia-X - European Association for Data and Cloud AISBL https://gaia-x.eu

DSBA - Data Spaces Business Alliance (Gaia-X, Big Data Value Association (BDVA), FIWARE Foundation, IDSA) https://data-spaces-business-alliance.eu

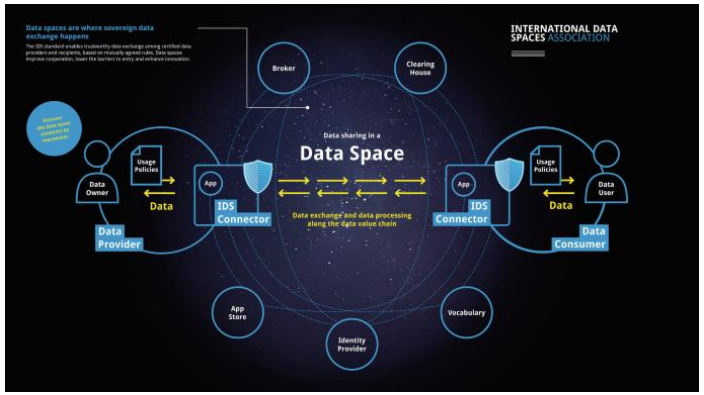
DSSC - Data Spaces Support Centre https://dssc.eu

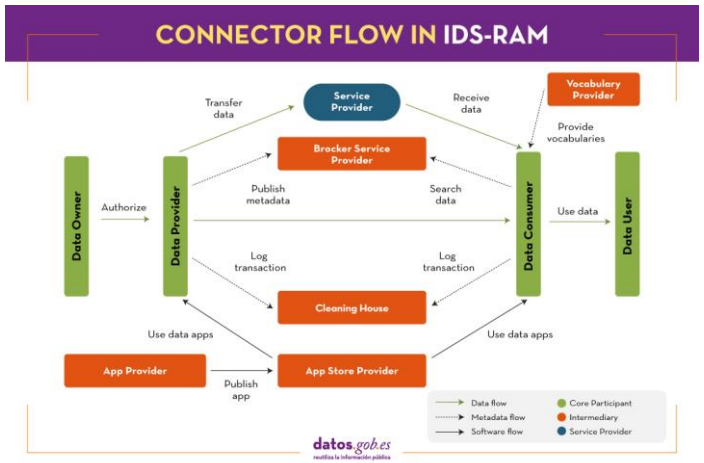
Oficina del Dato (Ministerio para la Transformación Digital y de la Función Pública, Secretaría de Estado de Digitalización e Inteligencia Artificial) https://oficinadato.gob.es https://datos.gob.es

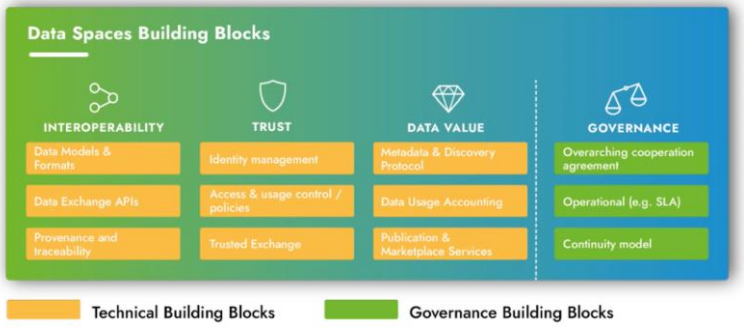
Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Convergencia e Interoperabilidad

Un camino necesario







Data Spaces Business Alliance

Unleashing the Data Economy

BDV BIG DATA VALUE ASSOCIATION · FIWARE FOUNDATION · gaia-x · INTERNATIONAL DATA SPACES ASSOCIATION

DATA SPACES SUPPORT CENTRE

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

DSBA - [‘Technical Convergence Discussion Document’ v2.0, 2023-04-21]

Seguridad

Empezando por el principio

La **seguridad informática**, también conocida como **ciberseguridad**,[1] es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la **información** contenida en una computadora o circulante a través de las redes de computadoras.[2] Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información. La ciberseguridad comprende *software* (**bases de datos**, **metadatos**, **archivos**), *hardware*, redes de computadoras, y todo lo que la organización entienda y valore como un riesgo si la información confidencial involucrada pudiera llegar a manos de otras personas, por ejemplo, convirtiéndose así en información privilegiada.

La definición de seguridad de la información no debe ser confundida con la de «seguridad informática», esta última solamente se encarga de la seguridad en el medio informático, pero por cierto, la información puede encontrarse en diferentes medios o formas, y no exclusivamente en medios informáticos.

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Seguridad

Legislación EU

Table 1: Overview of EU Legislation in the Digital Sector

Applicable law	Published in the Official Journal of the European Union
In negotiation	Proposal by the European Commission entered the legislative process.
Planed initiative	Mentioned by the European Commission as potential legislative initiative

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	General Data Protection Regulation (GDPR), (EU) 2016/679	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	Technology Transfer Block Exemption, (EC) 2014/316	Satellite and Cable I Directive, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Information Society Directive, (EC) 2001/29	Payment Service Directive 2 (PSD2), (EU) 2015/2366, 2023/0209(COD)
Regulation on a pilot regime distributed ledger tech. market, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Broadband Cost Reduction Directive, (EU) 2014/61, 2023/0046(COD)	Regulation on the free flow of non-personal data, (EU) 2018/1807	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on terrorist content online, (EU) 2021/784	Radio Equipment Directive (RED), (EU) 2014/53	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173	Open Internet Access Regulation, (EU) 2015/2120	Open Data Directive (PSI), (EU) 2019/1024	Directive on the protection of trade secrets, (EU) 2016/943	Information Security Regulation, 2022/0084(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)	Directive on Consumer Rights (CRD), (EU) 2011/83	P2B Regulation, (EU) 2019/1150	Portability Regulation, (EU) 2017/1128	Crypto-assets Regulation (MiCA), (EU) 2023/1114
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(NLE)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Data Governance Act (DGA Regulation), (EU) 2022/868	Standard essential patents, 2023/0133(COD)	Cybersecurity Regulation, 2022/0085(COD)	E-evidence Regulation, 2018/0108(COD)	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-Invoicing Directive, (EU) 2014/55	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	Satellite and Cable II Directive, (EU) 2019/789	Digital euro, 2023/0212 (COD)
	Decision on a path to the Digital Decade, (EU) 2022/2481	Roaming Regulation, (EU) 2022/612	ePrivacy Regulation, 2017/0003(COD)	Design Directive, 2022/0392(COD)	Cyber Resilience Act, 2022/0272(COD)	Digitalization of travel documents	General Product Safety Regulation, (EU) 2023/988	Geo-Blocking Regulation, (EU) 2018/302	Digital Market Act (DMA Regulation), (EU) 2022/1925	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205 (COD)
	European Chips Act (Regulation), 2022/0032(COD)	Regulation on the Union Secure Connectivity Programme, (EU) 2023/588	European Data Act (Regulation), 2022/0047(COD)	Compulsory licensing of patents, 2023/0129(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)		Machinery Regulation, (EU) 2023/1230	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560	European Media Freedom Act, 2022/0277(COD)	Payment Services Regulation, 2023/0210(COD)
	European critical raw materials act (Regulation), 2023/0079(COD)	.eu top-level domain Regulation, (EU) 2019/517	European Health Data Space (Regulation), 2022/0140(COD)				AI Act (Regulation), 2021/0106(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2023/1067		Revision of the late payments Directive
	Establishing the Strategic Technologies for Europe Platform (STEP), 2023/0199(COD)	New radio spectrum policy programme (RSPP 2.0)	Regulation on data collection for short-term rental, 2022/0358(COD)				Eco-design Regulation, 2022/0095(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
		Telecoms Act / Fair Share Initiative	Harmonization of GDPR enforcement 2023/0202(COD)				AI Liability Directive, 2022/0303(COD)	Right to repair Directive, 2023/0083(COD)	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		
			Interoperable Europe Act, 2022/0379(COD)					Political Advertising Regulation, 2021/0381(COD)			
			Access to vehicle data, functions and resources					Multimodal digital mobility services (MDMS)			
			GreenData4all					Consumer protection: strengthened enforcement cooperation			
								Consumer rights: adapting ADR to digital markets			

kaizenner.eu

bruegel

https://www.bruegel.org/sites/default/files/2023-07/Tables_Scott_Kai.pdf

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Seguridad

Legislación EU

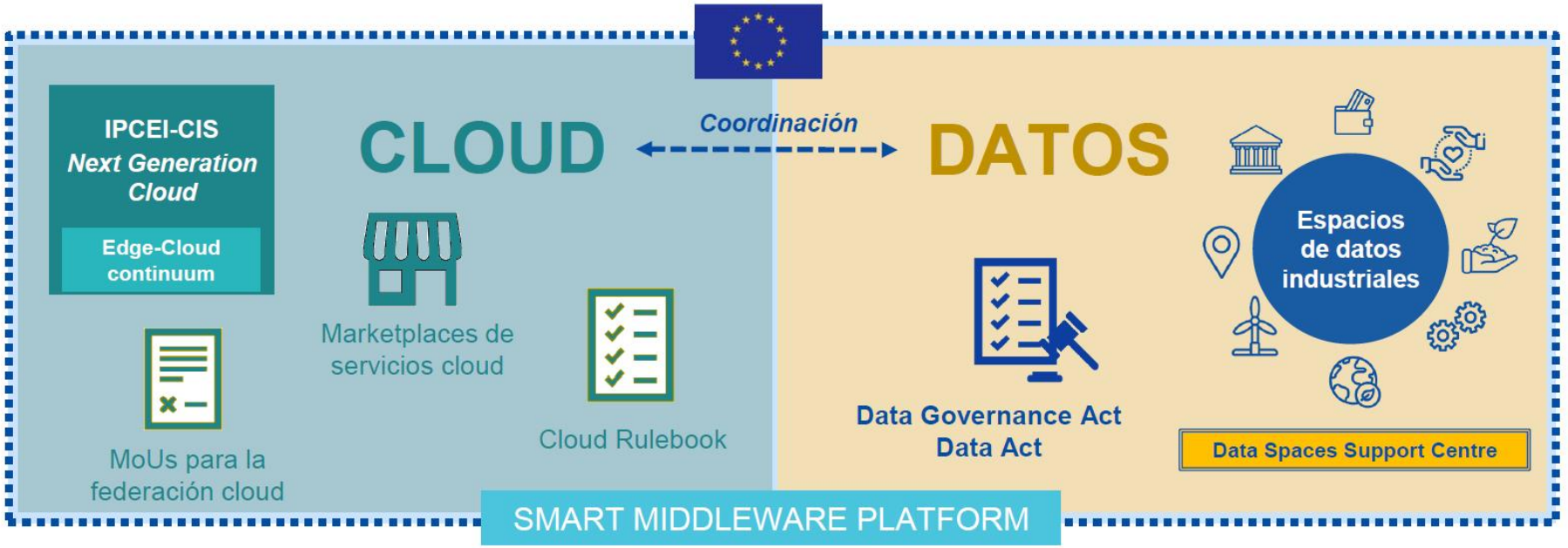
Table 1: Overview of EU Legislations in the Digital Sector

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	European Statistics, (EC) 2009/223, 2023/0237(COD)	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881 2023/0108(COD)	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	General Data Protection Regulation (GDPR), (EU) 2016/679	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	Toys Regulation, (EC) 2009/48, 2023/0290(COD)
Regulation on a pilot regime distributed ledger tech. market, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Broadband Cost Reduction Directive, (EU) 2014/61, 2023/0046(COD)	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa, (EU) 2019/817	European Standardization Regulation, (EU) 2012/1025
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173	Open Internet Access Regulation, (EU) 2015/2120	Regulation on the free flow of non-personal data, (EU) 2018/1807	Directive on the protection of trade secrets, (EU) 2016/943	Information Security Regulation, 2022/0084(COD)	Regulation on terrorist content online, (EU) 2021/784	eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Estrategia EU del dato

Oficina del Dato



4 PILARES:

Marcos de gobernanza para el acceso y uso de datos

Catalizadores e infraestructuras

Empoderamiento y aptitudes

Despliegue de espacios de datos industriales comunes

European Commission

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Definición de Espacio de Datos

Oficina del Dato desde fuentes EU

Los espacios de datos son el lugar ***donde desplegar*** la estrategia del dato UE.

Un espacio de datos es un ***ecosistema*** donde materializar la compartición voluntaria de los datos de sus participantes dentro de un entorno de ***soberanía, confianza y seguridad***, establecido mediante mecanismos integrados de gobernanza y técnicos, habilitadores de la generación de valor.

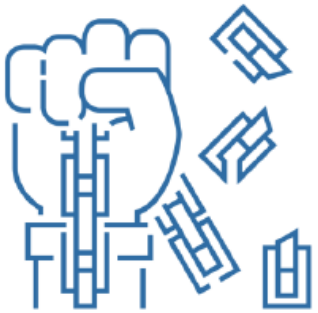
El espacio de datos facilitará encontrar, acceder y usar los datos, describiendo suficientemente los conjuntos de datos implicados y sus restricciones de uso, las estructuras de datos, vocabularios y taxonomías, así como los medios técnicos de acceso.

Habilita la ***generación sostenible de valor alrededor del dato***, catalizador de la innovación y el crecimiento empresarial, permitiendo identificar oportunidades de mercado, anticipar tendencias, tomar decisiones mejor informadas, aumentar la eficiencia operativa, desarrollar productos y servicios transformadores, o personalizar las experiencias de los clientes.

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Principios de diseño Espacios de Datos

(*) Open Dei. Data Spaces Design Principles.
Programa Horizon 2020



Soberanía de datos

Capacidad del dueño de los derechos de acceso y uso de los datos para definir las políticas de uso y acceso y que se garantice su cumplimiento (*enforcement*)

Apertura

Ausencia de barreras de entrada y salida.

Evitar los silos y la posición dominante.

Ecosistemas de oferta y demanda

Uso de estándares

Descentralización e interoperabilidad

Colección de dominios interoperables que cumplen con un conjunto de acuerdos funcionales, técnicos, operacionales, legales y económicos.

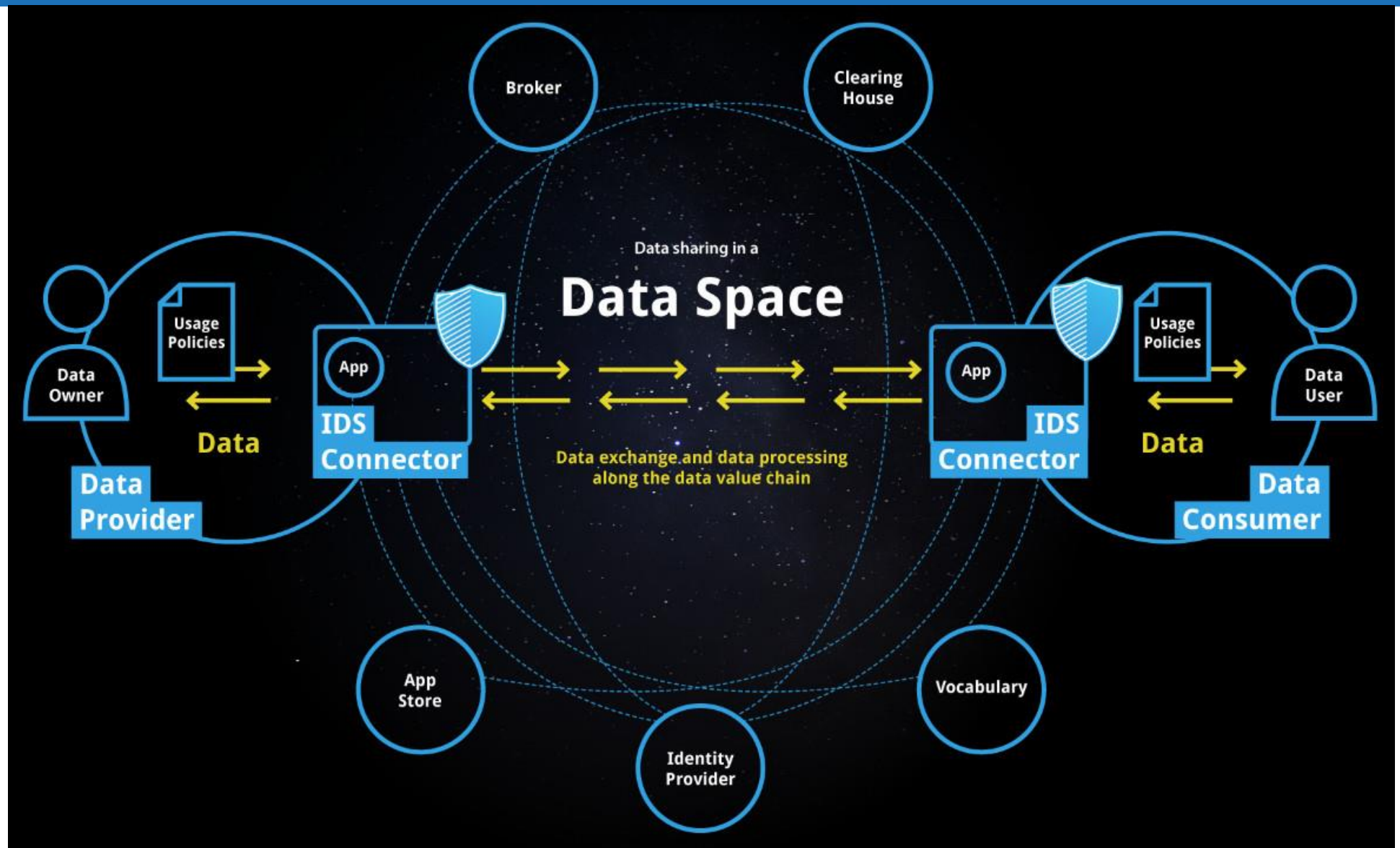
Gobernanza compartida

Gobernanza en la que todos los participantes se vean representados y se encuentren implicados.

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

¿Cómo es un Espacio de Datos?

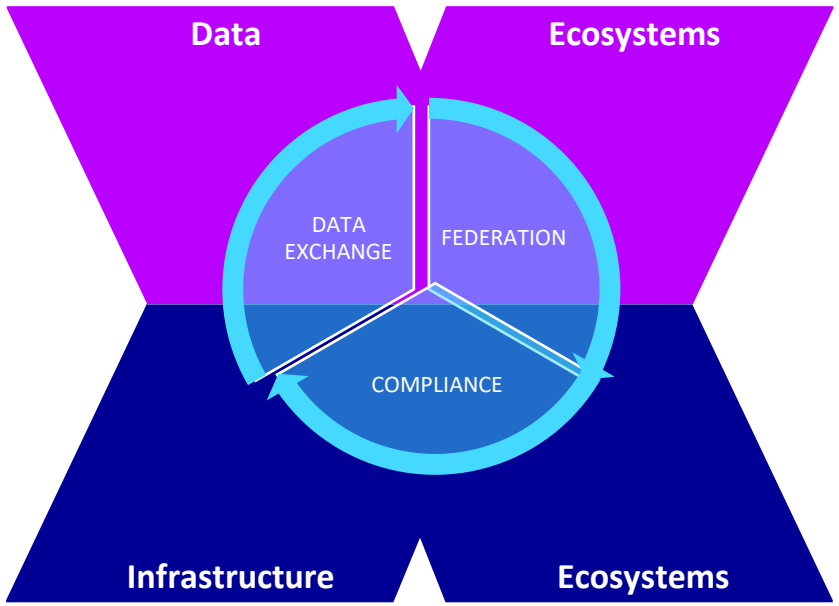
IDSA



Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

GAIA-X

A Federated and Secure Data Infrastructure



Advanced Services

New (Cross-) Sector Innovations / Applications buildfrom service composition.

Data Spaces / Federations

Interoperable & portable (Cross-) Sector data-sets and services.

Data Exchange

Anchored contract rules for access and data usage.

Gaia-X Compliance

Decentralized services to enable objective and measurable trust.

Label framework

Gaia-X and ecosystem specific Labels to ease market adoption through autonomy and self-determination.

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Espacios de datos compartidos

En resumen…

- Entornos técnicos completos
- Enfoque básico: compartir datos y **valorizarlo**
- Conservando la **soberanía** sobre ellos
- Condiciones técnicas y **normativas**
- **Confianza** en el intercambio de datos
- Proporcionar nuevos servicios (**nuevos negocios**)
- No se basan en ninguna infraestructura determinada (infraestructura previa)
- Módulos añadidos: probados y **certificados**
- Capacidad de **interconexión**, **interoperabilidad** semántica, visibilidad de los datos a los consumidores, según las condiciones estipuladas por quien ostente la soberanía.

- Los espacios de datos deben:
  - garantizar el intercambio de información (proveedores y consumidores)
  - de manera segura (confianza, privacidad)
  - las organizaciones deben de asegurar la privacidad y seguridad de los datos que almacenan y gestionan
  - garantías en el intercambio de información
  - determinar el cómo, cuándo y en qué condiciones se utilizan los datos

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

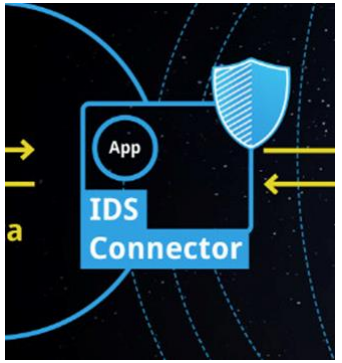
Conector como pieza central

Conector IDS

- El término conector procede del entorno de Industrial Data Spaces (IDS)
- El mismo término y concepto se utiliza en Gaia-X

- Es el elemento que conecta al espacio de datos la infraestructura/servicios de los consumidores y proveedores de datos.

- Definición de conector desde IDS (IDSA):
  - The IDS Connector is a dedicated software component that allows participants to attach usage ***policies*** to their ***data*** in a data space, ***enforce the usage*** policies and seamlessly ***track*** data provenance. The Connector acts as a gateway for data and services and as a trusted environment for apps and software.



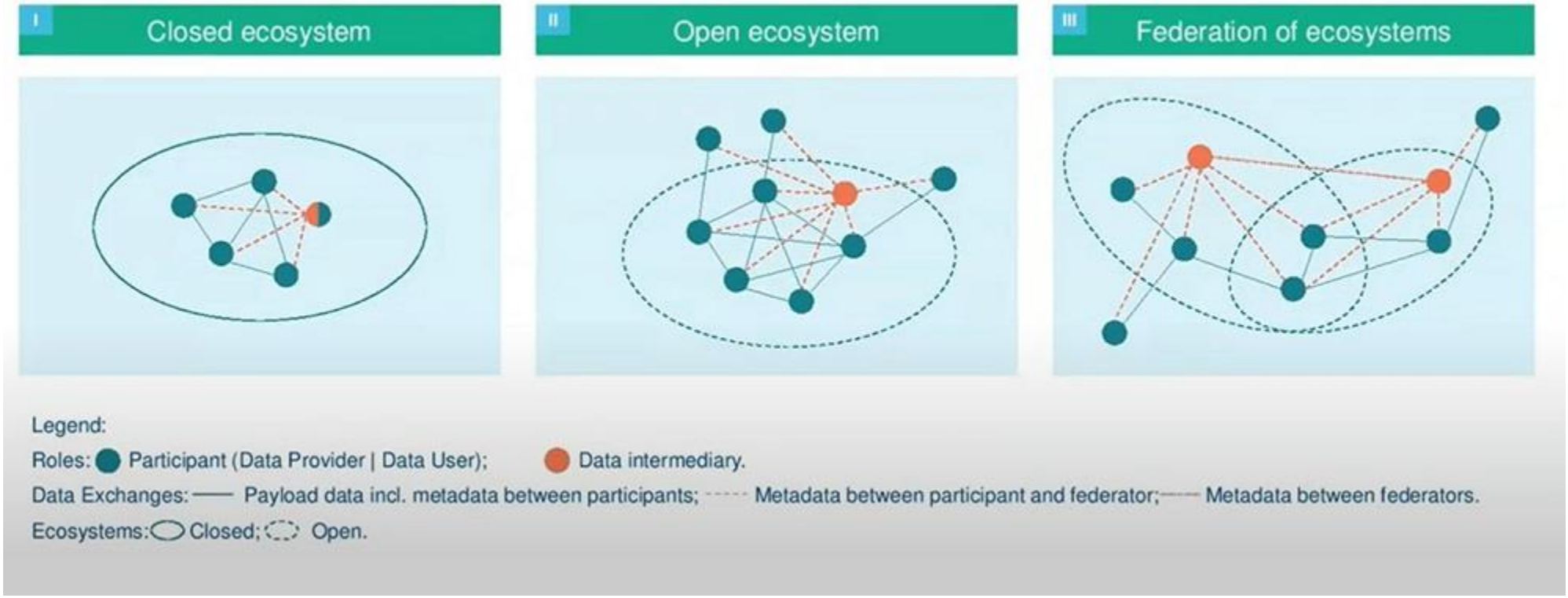
- El espacio de datos contará con otros elementos, comunes a todo el espacio de datos, operados por la ***Autoridad del Espacio de Datos*** y/o por operadores específicos: Broker, Clearing House, App Store, Identity Provider, Vocabulary (obligatorios/opcionales).

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Federación de Espacios de Datos

Más allá de la arquitectura IDS

Expansión de los espacios de datos hacia la ***federación***.



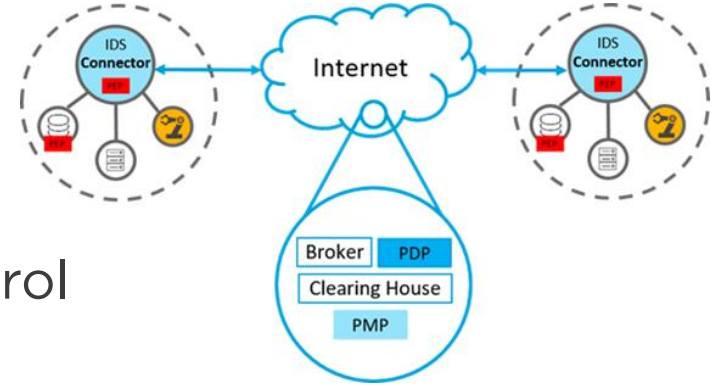
https://datos.gob.es/es/noticia/webinar-europeo-sobre-novedades-en-los-espacios-de-datos-del-futuro

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Claves en la arquitectura IDS

La seguridad en la arquitectura

- Requisito estratégico: ***proporcionar cadenas de suministro de datos seguras***.
- Establecer y mantener la ***confianza*** (trust) entre los participantes
- Arquitectura de seguridad IDS: en su arquitectura IDS especifica elementos al cargo de la seguridad (medios para identificar dispositivos, proteger transacciones e intercambio de datos, control del uso de los datos
- ***No*** se proporcionan servicios específicos o herramientas de seguridad o ciberseguridad en general.
- Se debe considerar al ***diseñar*** y desarrollar el software
- Aspectos no funcionales incluidos: la seguridad y la confianza sirven como habilitadores de funcionalidades como el intercambio de datos.
- La seguridad se trata como un requisito transversal de las capas del modelo de arquitectura de referencia (IDS-RAM).



Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Aspectos de seguridad y modelo de confianza

En IDSA-RAM

- Permitir o restringir transacciones u operaciones
- Ofrecer ***datos confidenciales a socios comerciales confiables***.
- Identificación y autenticación confiables de los componentes mediante una infraestructura de clave pública (PKI).
- Autoridad de certificación (CA) como elemento obligatorio en el espacio de datos (claves, certificados).
- Servicio de aprovisionamiento de atributos dinámicos (DAPS) (tokens de atributos dinámicos)
- Proceso de ***certificación*** de los conectores (verificación de las especificaciones de seguridad identificadas en DIN SPEC 27070, familia de estándares de seguridad de IEC62443-4-2)

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Aspectos de seguridad y modelo de confianza

IDS-RAM: Perspectiva de seguridad

IDS-RAM especifica tres perspectivas a modo de referencia: Seguridad, Certificación y Gobernanza.

Todos los **aspectos de seguridad** en la IDS-RAM se pueden consultar en su especificación: https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0/tree/main/documentation/4_Perspectives_of_the_Reference_Architecture_Model/4_1_Security_Perspective

- Security Aspects addressed by the different layers (business, functional, information, process, system)
- Identity and Trust Management
- Securing the Platform
- Securing Applications
- Securing Interaction between IDS Components
- Data Usage Control
- Data Provenance Tracking

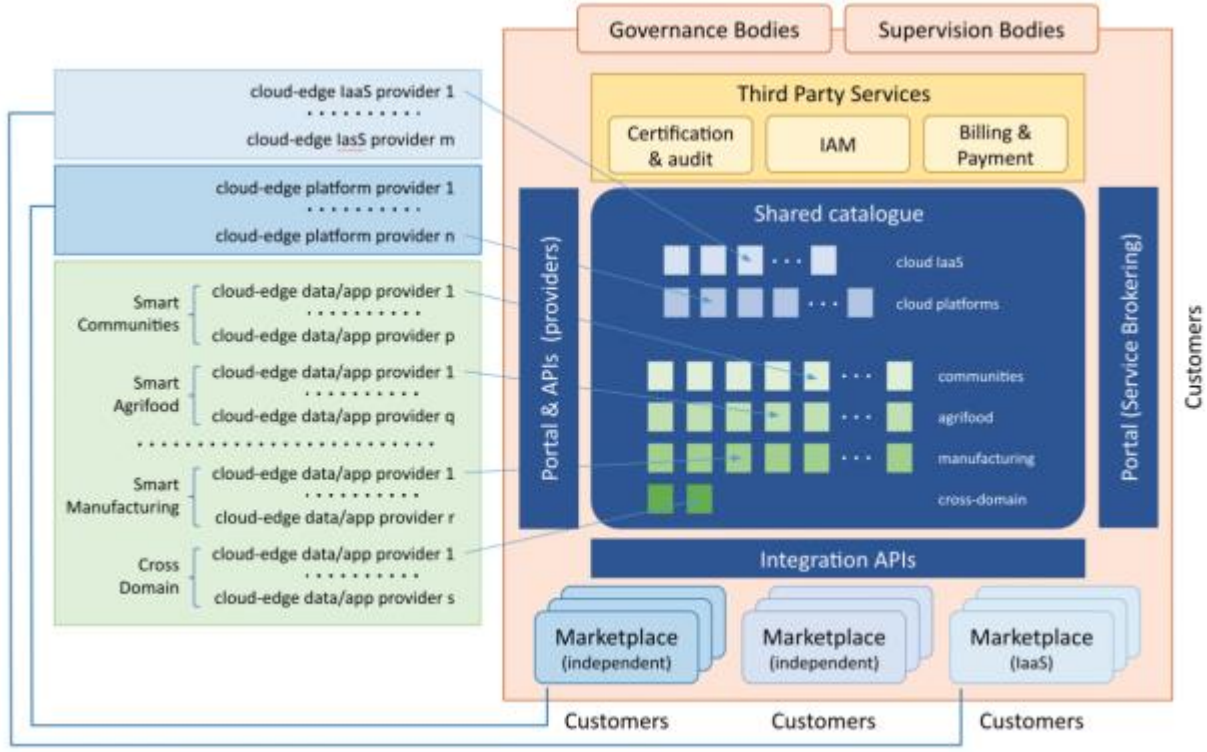
Aspecto Funcional IDS (IDS-RAM v4)

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Evolución de los espacios de datos hacia su federación

IDS y Gaia-X

- Espacios de datos ***federados***.
- Ampliar las posibilidades de uso / compartición de datos.
- Gaia-X:
  - Marco de Anclaje de Confianza (Trust Anchor Framework)
  - Marco de Gestión de Identidad y Acceso Descentralizado
  - MAC (TAF) define y obliga a un conjunto de reglas que las diferentes organizaciones acuerdan seguir
  - ***Self-descriptors*** para los participantes y los proveedores de servicios



*Decentralized Open **Marketplace** Ecosystem **DOME** (Fuente: DSBA)*

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

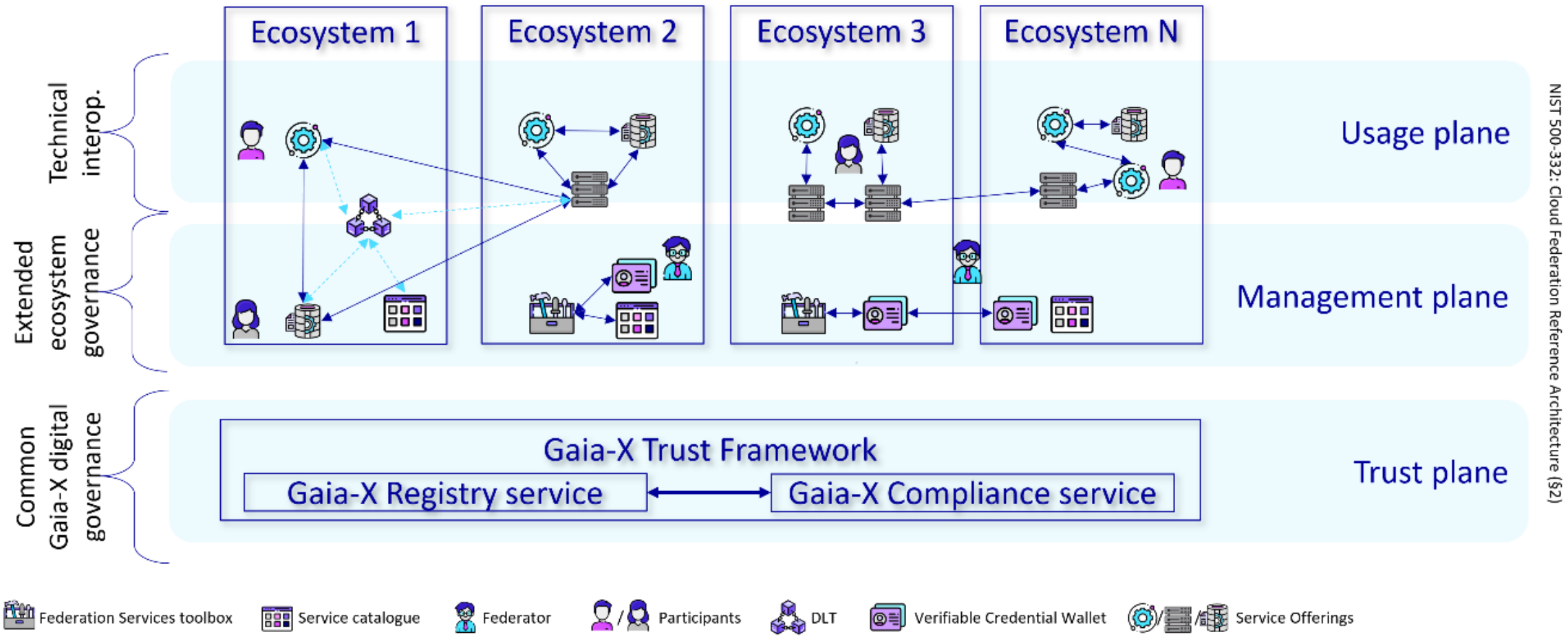
Características del servicio de conformidad de Gaia-X

Resumen

- Verificar el cuerpo de ***autodescripción*** de un participante o servicio de acuerdo con el marco de confianza.
- Verificar las ***firmas*** de autodescripción y las ***credenciales*** provenientes de trust anchors.
- Proporcionar una autodescripción canonizada y normalizada para la prueba de conformidad.
- Añadir una prueba de cumplimiento y emisión de ***Credencial Verificable*** (VC).
- Verificar de VC (verified credential, autodescripción firmada, incluida la prueba de cumplimiento).
- El servicio se puede utilizar a través de API y Swagger UI.

Expectativas Gaia-X

Marco de confianza, características



Escenario de **compartición de datos en espacios federados** (Fuente: Gaia-X ASIBL)

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Carencias de desarrollo

Marco de Anclaje de Confianza TAF

- ***Vinculación de ID***: ¿Cómo verificar que un identificador dado corresponde a una identidad legal válida de una entidad en el mundo real?

- ***Prueba de participación***: ¿Cómo verificar que la entidad es confiable porque es un participante suscrito en un ecosistema determinado (por ejemplo, para verificar la confianza del Catálogo Compartido de Especificaciones de Productos y de Ofertas de Productos)?

- ***Prueba de Autoridad Emisora***: ¿Cómo comprobar que las credenciales presentadas por un participante hayan sido emitidas por otra entidad que pueda ser considerada Emisora de Confianza de ese tipo de credenciales? Esto permite que el verificador deposite la confianza adecuada en los hechos atestiguados por las Credenciales Verificables presentadas por un participante.

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Carencias de desarrollo

Administración de identidad y acceso descentralizado

- ***Identificación***: ¿Cómo verificar que un identificador enviado por un participante a otra entidad ha sido enviado por el participante y no por un impostor que conoce el identificador? Además, necesitamos vincular criptográficamente el identificador a las Credenciales Verificables enviadas por el participante para que los hechos atestiguados en las credenciales puedan usarse para autenticación y autorización.

- ***Autorización***: ¿Cómo usar los hechos certificados en las Credenciales verificables presentadas por un participante para realizar un control de acceso avanzado de RBAC/ABAC y aplicación de políticas?

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Carencias de desarrollo

Aproximaciones y propuestas en curso

- Identificadores = certificados digitales emitidos por los ***Proveedores de Servicios de Confianza*** (TSP) autorizados por las leyes europeas.
- Combinación con ***credenciales y presentaciones verificables***: facilita la validación transfronteriza de firmas electrónicas, sellos electrónicos y más. Se firmarán mediante certificados digitales.
- Enfoque para las ***personas físicas*** y enfoque para las ***personas jurídicas***. Se deben de cubrir ambos.
- ***Lista de participantes de confianza***: identidades y los metadatos asociados participan en el ecosistema concreto.
- Actualmente, el conector se identifica mediante los atributos de un certificado X.509.
    - Basado en DID (identificador descentralizado, según esquema URI [universal resource identifier] de W3C).
    - Perfil de seguridad validado por una agente de evaluación externa y proporcionado a una autoridad central, pero el flujo de trabajo de proporcionar la asignación directamente como VC/VP debe describirse en detalle. Más aún para contemplar su ***federación***.

Oportunidades de negocio y mensajes para los primeros receptores

Oficina del dato – Actores en un espacio de datos

- ***Promotor del espacio de datos***

  Es el impulsor del entorno de compartición y explotación, responsable de su gobierno y gestión. Generador de comunidad, articulando diferentes modelos de negocio y buscando y atrayendo nuevos participantes

- ***Proveedor tecnológico***

  Encargado de integrar y operar la solución técnica que permita el despliegue de la infraestructura del espacio de datos. Realiza el desarrollo, configuración y parametrización de la solución técnica basada en una arquitectura de referencia que permite desplegar el espacio de datos.

- ***Consumidores de servicios de datos***

  Consumen servicios de datos (productos de datos) dentro del contorno de derechos y obligaciones del espacio de datos. Incorpora a su sistema el valor del dato ajeno, de diferentes proveedores, conjugándolo con el dato propio.

- ***Proveedores de servicios de datos***

  Ofrecen servicios de datos (productos de datos) dentro del contorno de derechos y obligaciones del espacio de datos.

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

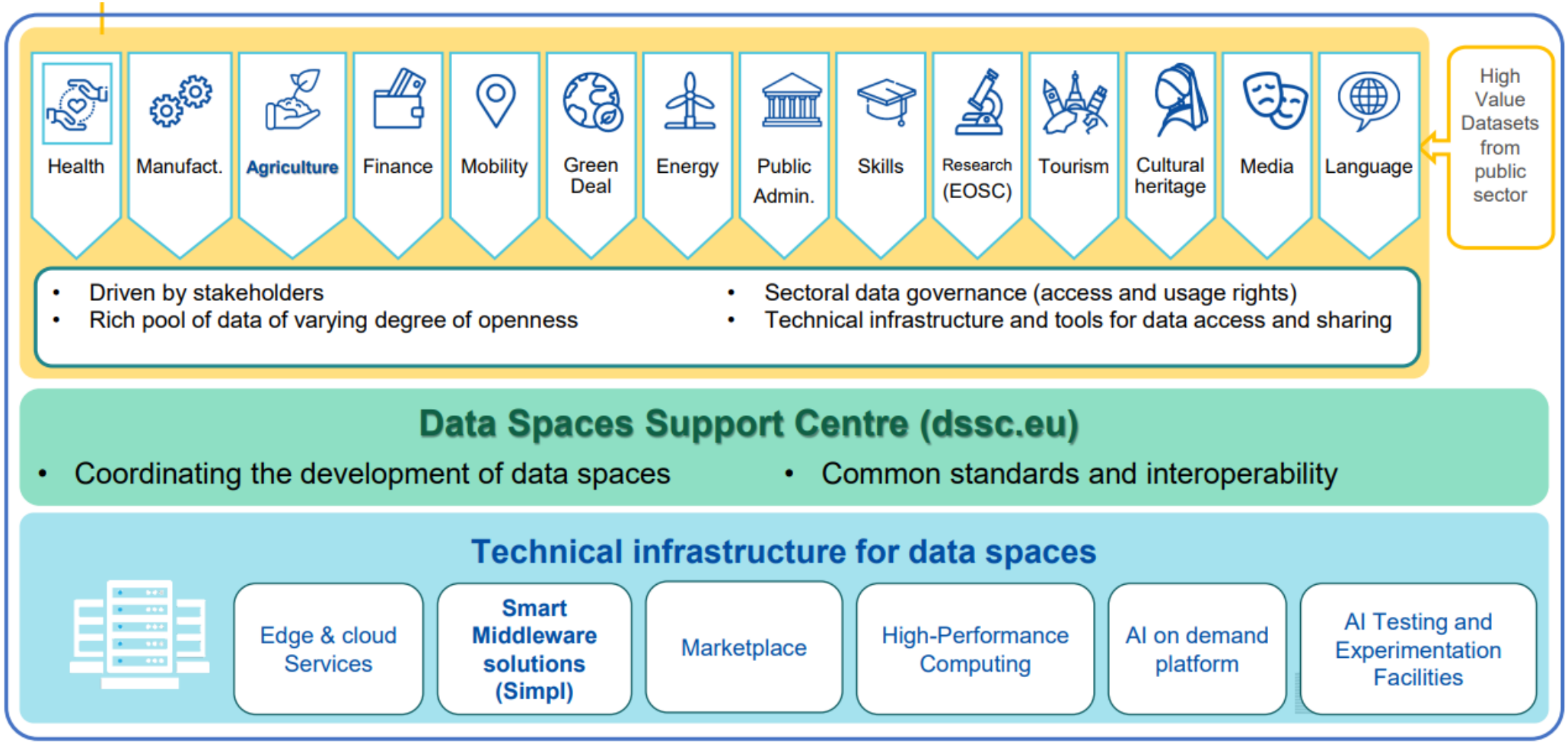
Oportunidades de negocio y mensajes para los primeros receptores

Comisión Ciberseguridad

- Notable cantidad de aspectos por resolver e implementar (grupos operativos de Gaia-X, DSSC y otras entidades).
- Abiertos a la participación de los agentes que lo deseen.
- La arquitectura propuesta (DOME) proporcionará medios para la integración de servicios de terceros, que pueden resultar de interés para empresas del sector de ciberseguridad y conformidad:
  - ***Servicios de agencias de certificación y auditoría*** que ayuden a validar la confiabilidad, seguridad y soberanía de ciertos servicios en la nube mediante la comprobación y verificación de su cumplimiento con certificaciones predeterminadas en todo el mercado.
  - ***Proveedores de servicios de IAM*** (identity and access management) que ofrezcan servicios alineados con estándares abiertos para IAM adoptados en DOME, brindando a los participantes la capacidad de administrar de manera segura identidades y acceder a servicios específicos de aplicaciones y datos en la nube y perimetrales.
  - ***Proveedores de servicios de facturación y pago*** que funcionan como puertas de enlace que se basan en registros de transacciones registrados en la infraestructura de red de cadena de bloques federada subyacente a DOME, para proporcionar facturación segura, transparente y confiable a los consumidores y pago a los proveedores.

Iniciativas europeas de Espacios de datos

Oficina del dato - EU Digital Strategy



Second staff working document on data spaces 2024 01 24

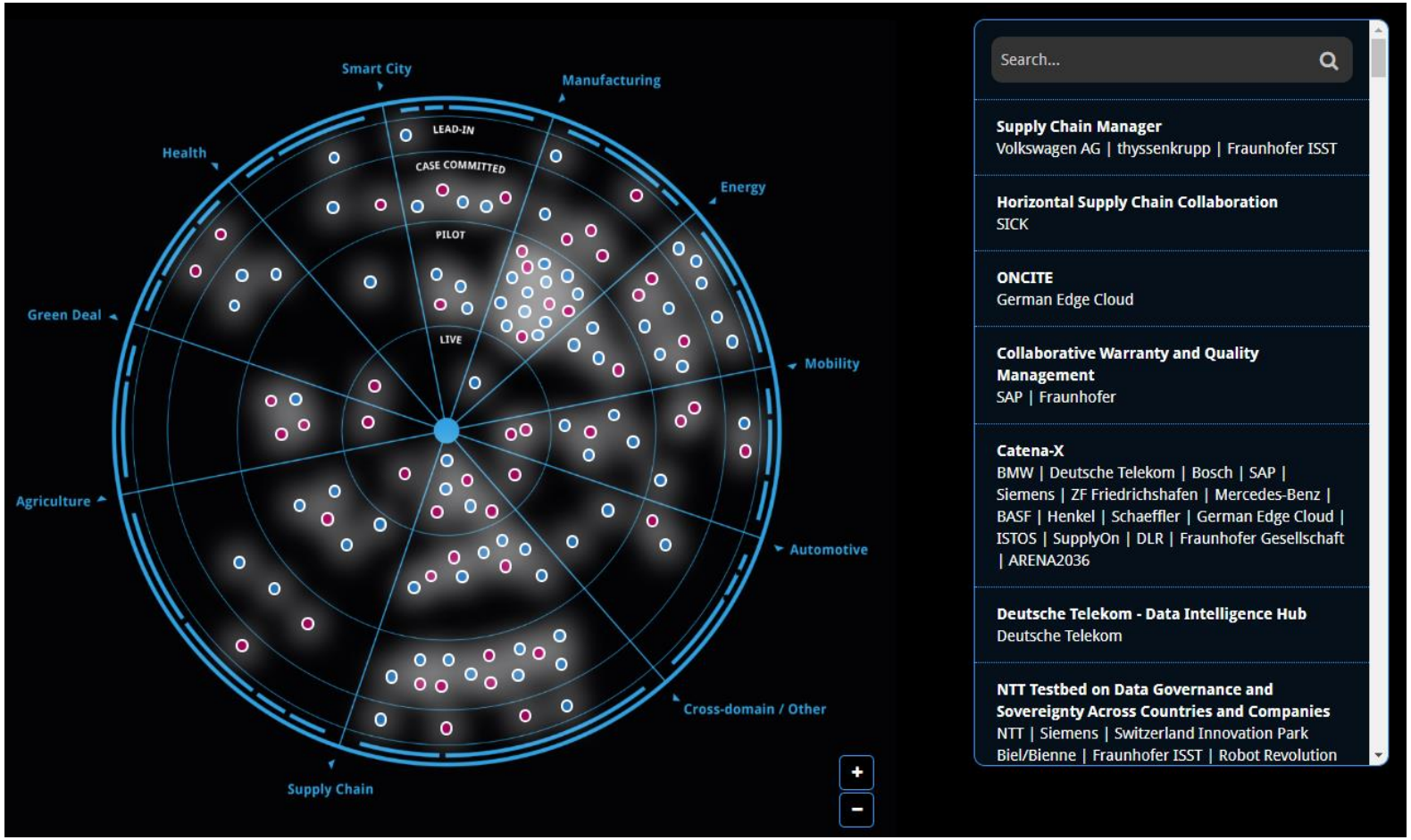
https://digital-strategy.ec.europa.eu/en/library/second-staff-working-document-data-spaces

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Radar de Espacios de Datos

IDSA Data Spaces Radar

- Radar de Espacios de Datos actual en IDSA: https://internationaldataspaces.org/adopt/data-spaces-radar/
- Evolución y nuevas funcionalidades en desarrollo: https://www.dataspaces-radar.org/



Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

¡Muchas gracias!

Para cualquier consulta o más información:

wwww.ametic.es

ametic@ametic.es

@AMETIC_es #AMETIC