BAIDATA

INTERNATIONAL DATA SPACES ASSOCIATION

Pasaporte Digital de Producto: Arquitectura Y Recomendaciones Clave

Análisis y Comentarios sobre el documento "D4.1 Reference Architecture" del proyecto CIRPASS 2

CIRPASS 2
Digital Product Passport

Título del Documento: Pasaporte Digital de Producto: Arquitectura y Recomendaciones Clave

Subtítulo: Análisis y Comentarios sobre el documento “D4.1 Reference Architecture” del proyecto CIRPASS 2

Versión: 1.0

Fecha de Publicación: Junio de 2025

Publicado por: BAIDATA

Autores:
- Jesús Alonso (BAIDATA)
- Cristina Urizar (BAIDATA)
- Naia Galán (BAIDATA)

Descargo de Responsabilidad: El contenido de este documento se fundamenta en el entregable D4.1 Reference Architecture del proyecto CIRPASS 2. Las interpretaciones y comentarios aquí vertidos son responsabilidad exclusiva de los autores y no representan necesariamente la postura oficial de CIRPASS 2 ni de la Unión Europea.

Tabla de contenido

FICHA TÉCNICA 6
¿Qué es este documento? 6
¿Qué encontraré en este documento? 6
¿Por qué y para quién es interesante este documento? 6

RESUMEN EJECUTIVO 7

1. Introducción 8
1.1. El alcance de esta arquitectura: Lo que encontrará y lo que no 8
1.2. Principios rectores: La filosofía detrás del diseño del DPP 10
1.3. Roles clave en el ecosistema del DPP: ¿quién es quién en el mundo del DPP? 11
1.4. Estructura del documento: navegando los fundamentos del DPP 12

2. Bloques de construcción 13
2.1. Operador económico responsable (rEO) 13
2.2. Autoridades públicas 16
2.3. Proveedor de servicios de DPP (DPPSP) 18
2.4. Usuario final y Operador independiente (End User and Independent Operator) 19
2.5. Agencia de credenciales y agencia emisora (Credentials Agency and Issuing Agency) 20
2.6. Otros actores, incluidos los actores de la cadena de suministro (Other Actors, Including Supply Chain Actors) 21

3. Recomendaciones arquitectónicas clave 23
3.1. Interoperabilidad 23
3.2. Gestión de identidad y acceso 24
3.3. Integridad del DPP 25
3.4. Acceso al DPP 26
3.5. Gestión de datos 26
3.6. Visualización 27

4. Riesgos y mitigaciones 29
4.1 Tipos de Riesgos Técnicos Identificados 29
4.2 Estrategias de Mitigación 29

Tablas y Figuras

Figura 1. Contexto del documento en el marco del proyecto CIRPASS 2 8
Figura 2. Una visión basada en roles del ecosistema del DPP 11
Figura 3. Bloques de construcción desde la perspectiva del REO 13
Figura 4. Bloques de construcción desde la perspectiva de las Autoridades Públicas 16
Figura 5. Bloques de construcción desde la perspectiva de los proveedores de servicios de DPP 18
Figura 6. Bloques de construcción desde la perspectiva de los usuarios finales y los operadores independientes 19
Figura 7. Bloques de construcción desde la perspectiva de la agencia de credenciales y la agencia emisora 20
Figura 8. Bloques de construcción desde la perspectiva de otros actores 21
Figura 9. Recomendaciones de interoperabilidad 23
Figura 10. Estructura de plantillas anidadas de CIRPASS 2 24
Figura 11. Recomendaciones de gestión de identidad y acceso 24
Figura 12. Recomendaciones de gestión de integridad del DPP 25
Figura 13. Recomendaciones de gestión de acceso al DPP 26
Figura 14. Recomendaciones de gestión de acceso al DPP 27
Figura 15. Recomendaciones de gestión de visualización 28

FICHA TÉCNICA

¿Qué es este documento?

Este documento, el entregable D4.1 “Reference Architecture v1.0” del proyecto CIRPASS 2, es la **definición fundamental de la arquitectura de referencia del Pasaporte Digital de Producto (DPP)**. Detalla los principios, componentes y flujos esenciales que permitirán el funcionamiento armonizado del sistema DPP en Europa. Es, en esencia, el plano tecnológico de cómo se construirá y operará el DPP.

Para BAIDATA, participar en este nivel de definición asegura que las necesidades de nuestras empresas asociadas sean consideradas desde las primeras etapas.

¿Qué encontraré en este documento?

Aquí descubrirás **los pilares técnicos** sobre los que se asienta el DPP. El documento explora los principios generales que rigen su diseño, identifica los **actores y roles clave** en el ecosistema (fabricantes, proveedores de servicios DPP, autoridades, etc.), y describe los **bloques de construcción esenciales** (como los sistemas de identificación, los servicios de datos y los registros de la UE). También se profundiza en los **flujos de datos** críticos y se presentan **componentes avanzados** que permitirán funcionalidades futuras, así como los **requisitos no funcionales** (seguridad, escalabilidad, interoperabilidad) que aseguran un sistema robusto y fiable.

¿Por qué y para quién es interesante este documento?

Este documento es de interés fundamental para:

- **Empresas Tecnológicas (especialmente pymes y startups):** Proporciona la base para el desarrollo de soluciones y servicios compatibles con el DPP, abriendo **nuevas oportunidades de negocio e innovación** en la gestión y compartición de datos de producto. Es la guía para construir el futuro digital.

- **Empresas Usuarias (a través de clústeres y asociaciones empresariales):** Permite comprender cómo el DPP impactará sus cadenas de valor, cómo podrán **acceder y compartir datos** de forma soberana, y cómo la transparencia mejorará sus operaciones y la sostenibilidad.

- **Administraciones Públicas (regionales y locales):** Ofrece una visión clara de la infraestructura técnica necesaria para la implementación y el control de las regulaciones del DPP, facilitando la **coordinación de iniciativas** y el acceso a la información relevante.

Para todos ellos, BAIDATA facilita el **acceso y la interpretación** de esta arquitectura, promoviendo el conocimiento y la colaboración para que nuestros socios puedan **liderar la adopción y el desarrollo del DPP** en el contexto de la economía del dato.

Recuerde que este documento es un extracto del informe original publicado por el proyecto CIRPASS 2 “D4.1 – Reference Architecture v1.0”. Puede consultar el documento original en el siguiente enlace: **https://cirpass2.eu/project-results/**

RESUMEN EJECUTIVO

El presente documento es un extracto del entregable D4.1 del proyecto CIRPASS 2, que recoge la **Arquitectura de Referencia del Pasaporte Digital de Producto (DPP)**. Esta arquitectura no es solo un conjunto de especificaciones técnicas; es el **plano fundamental** que guiará el desarrollo y la implementación de un ecosistema de DPP armonizado, interoperable y escalable en toda Europa. Su objetivo principal es asegurar la **transparencia y la sostenibilidad** a lo largo del ciclo de vida de los productos, desde su diseño hasta su fin de vida, y facilitar la **compartición segura y soberana de datos** para impulsar la economía circular.

En sus páginas, se detallan los **principios rectores** que aseguran la consistencia y la interoperabilidad de los DPP, así como los **actores y roles clave** involucrados en este ecosistema digital (desde fabricantes y operadores económicos hasta proveedores de servicios y autoridades públicas). El documento también profundiza en los **bloques de construcción esenciales** del sistema DPP, incluyendo los sistemas de identificación global de productos y participantes, los servicios de datos que permiten el acceso a la información del DPP, y los mecanismos de interoperabilidad para la resolución de identificadores. Se describen también los **flujos de datos** críticos y se abordan componentes avanzados para futuras funcionalidades, así como los **requisitos no funcionales** (seguridad, escalabilidad, privacidad y fiabilidad) que son vitales para la confianza y la adopción masiva del sistema.

Para BAIDATA y su comunidad, esta arquitectura es de una **importancia estratégica** vital. No es meramente un documento técnico, sino la hoja de ruta que permitirá **construir y aprovechar nuevas oportunidades de negocio, optimizar operaciones y desarrollar modelos de valor añadido** basados en el dato. Comprenderla es esencial para las empresas que buscan innovar, diferenciarse y liderar en este nuevo paradigma de la economía del dato.

Como asociación BAIDATA, nuestro compromiso es impulsar la economía del dato y la implementación del Pasaporte Digital de Producto (DPP), facilitando a sus socios el acceso al conocimiento, la promoción de la innovación y la creación de un ecosistema colaborativo para liderar estas nuevas oportunidades de negocio.

1. INTRODUCCIÓN

En un panorama europeo que avanza hacia una economía circular y más transparente, la gestión de datos se ha convertido en un pilar fundamental. Es en este contexto que iniciativas como el **Pasaporte Digital de Producto (DPP)** adquieren una relevancia estratégica innegable. Este documento, un extracto y análisis del entregable D4.1 "Reference Architecture v1.0" del proyecto CIRPASS 2, es una **guía esencial** para comprender los fundamentos técnicos y conceptuales que sustentarán el ecosistema del DPP.

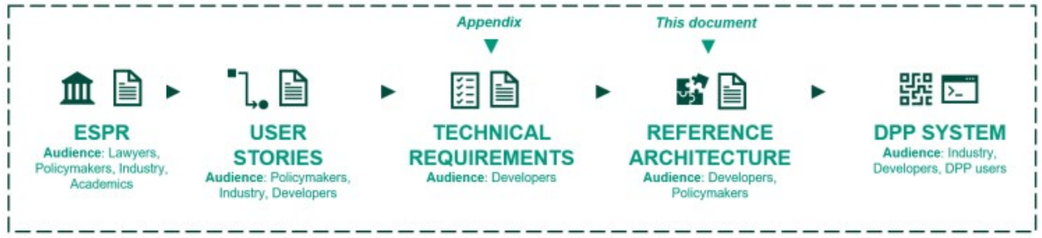

Figura 1. Contexto del documento en el marco del proyecto CIRPASS 2

El proyecto **CIRPASS 2**, cofinanciado por la Unión Europea, es una pieza clave en este esfuerzo. Su misión es precisamente desarrollar y probar los elementos esenciales del DPP, con un enfoque prioritario en la **definición de una arquitectura de referencia sólida**. Esta arquitectura es el eslabón fundamental que conecta las ambiciones regulatorias del **Reglamento de Ecodiseño de Productos Sostenibles (ESPR)** –la fuerza motriz detrás del DPP– con el desarrollo técnico y los esfuerzos de estandarización. A través de este documento, buscamos desmitificar este plano técnico, haciéndolo accesible y relevante para la comunidad de BAIDATA, que se sitúa en el centro de la promoción de la economía del dato y los espacios de datos en la península ibérica.

1.1. El alcance de esta arquitectura: Lo que encontrará y lo que no

Esta Arquitectura de Referencia del Pasaporte Digital de Producto (DPP) es un documento fundamental que sienta las bases para un futuro ecosistema de datos de producto armonizado. Su objetivo es proporcionar una guía clara y una visión estructurada de cómo **debería ser un sistema DPP funcional y coherente a nivel europeo**.

En este extracto del entregable D4.1, usted encontrará una exploración detallada de:

- **Bloques de Construcción Esenciales:** Los componentes fundamentales y las funcionalidades que conforman el sistema DPP, desde la identificación unívoca de productos y actores, hasta los servicios de datos y la interoperabilidad para el intercambio de información. Se examinan las interfaces y los mecanismos de comunicación necesarios entre estos bloques.

- **Recomendaciones para el Diseño:** Este documento no solo describe, sino que también ofrece directrices y consideraciones clave para el diseño y la implementación de soluciones DPP, buscando maximizar la eficiencia, la seguridad y la usabilidad.

- **Gestión de Riesgos y Desafíos:** Se identifican los posibles riesgos inherentes a la implementación de un sistema de esta envergadura y se proponen enfoques para mitigarlos, asegurando un camino más seguro hacia la adopción del DPP.

- **Estructura y Apéndices:** Se explica cómo el documento está organizado para facilitar su comprensión, incluyendo referencias a apéndices que ofrecen detalles técnicos adicionales sobre aspectos como la resolución de identificadores y los esquemas de información clave.

¿Qué no cubre esta Arquitectura de Referencia? Es importante señalar que este documento se centra en el **marco técnico y conceptual**. Por ello, deliberadamente **no abarca** los siguientes aspectos:

- **Actos Delegados Específicos:** No define los requisitos detallados de información que serán obligatorios para grupos de productos específicos, los cuales se establecerán mediante los Actos Delegados de la Comisión Europea.

- **Modelos de Gobernanza:** No profundiza en los aspectos de gobernanza, legales o de negocio específicos que cada sector o iniciativa deberá desarrollar para operar los espacios de datos del DPP.

- **Implementaciones Concretas:** No proporciona una implementación de software lista para usar, sino un marco de alto nivel para guiar futuros desarrollos.

1.2. Principios rectores: La filosofía detrás del diseño del DPP

La Arquitectura de Referencia del Pasaporte Digital de Producto (DPP) no ha sido diseñada al azar. Se fundamenta en un conjunto de principios rectores que aseguran su eficacia, resiliencia y su capacidad para adaptarse a las necesidades futuras de la economía circular. Comprender estos principios es esencial para cualquier entidad que desee contribuir al ecosistema del DPP o desarrollar soluciones compatibles.

Estos son los principios clave que guían el diseño de la arquitectura del DPP:

- **Orientación a la Demanda y al Valor:** La arquitectura se centra en las necesidades reales de los usuarios (empresas, consumidores, autoridades) y en la generación de valor tangible, impulsando la adopción y la utilidad del DPP en el mercado.

- **Interoperabilidad por Diseño:** Reconociendo la diversidad de sectores y sistemas, la arquitectura está concebida para permitir el intercambio de datos fluido y la comunicación efectiva entre diferentes implementaciones del DPP, tanto a nivel técnico como semántico.

- **Escalabilidad y Flexibilidad:** El sistema está diseñado para manejar un volumen masivo de DPPs y transacciones, permitiendo su expansión y adaptación a nuevas regulaciones, tecnologías y casos de uso futuros, garantizando su relevancia a largo plazo.

- **Seguridad, Privacidad y Confianza:** Estos principios son fundamentales. La arquitectura integra mecanismos robustos para asegurar la protección de los datos sensibles, garantizar la privacidad de los usuarios y establecer un marco de confianza para la compartición de información.

- **Sostenibilidad y Eficiencia en los Recursos:** La arquitectura busca optimizar el uso de recursos tecnológicos, reduciendo el impacto ambiental de las infraestructuras digitales y promoviendo prácticas que apoyen los objetivos de la economía circular.

- **Transparencia y Trazabilidad:** Facilita la visibilidad sobre el origen, la composición y el ciclo de vida de los productos, permitiendo una mayor rendición de cuentas y apoyando decisiones informadas.

Estos principios no solo definen el marco técnico, sino que también reflejan los valores intrínsecos del proyecto CIRPASS 2 y la visión de la Unión Europea para una economía del dato más abierta, segura y sostenible.

1.3. Roles clave en el ecosistema del DPP: ¿quién es quién en el mundo del DPP?

La implementación efectiva del Pasaporte Digital de Producto (DPP) requiere la participación y la colaboración de una variedad de actores, cada uno con responsabilidades y funciones específicas dentro del ecosistema. Comprender estos roles es fundamental para que las empresas y organizaciones identifiquen su posición, sus obligaciones y las oportunidades de interacción en este nuevo panorama de datos.

Este documento, en línea con las definiciones establecidas en las “User Stories v3” de CIRPASS 2, identifica y describe los roles principales:

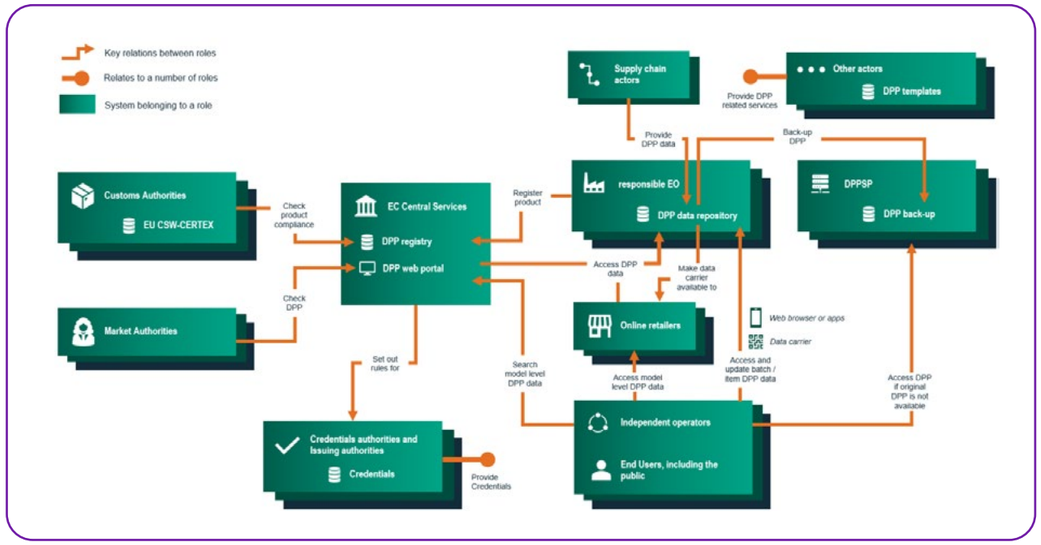

Figura 2. Una visión basada en roles del ecosistema del DPP

En el contexto de la arquitectura del DPP, los principales actores y roles que operan en este ecosistema son:

- **Operador económico responsable (rEO - responsible Economic Operator):** Se refiere a una persona jurídica que es responsable de crear un DPP y de todas las obligaciones legales que conlleva.

- **Usuario final (End User):** Una persona física o jurídica en la UE a quien se le ha puesto un producto a su disposición.

- **Operador independiente (Independent Operator):** Son personas físicas o jurídicas que realizan actividades asociadas con la Economía Circular (es decir, actividades de la “R-Ladder” como reparar, remanufacturar, reciclar).

- **Proveedor de servicios de DPP (DPPSP - DPP Service Provider):** Se refiere a una persona física o jurídica autorizada por el rEO para proporcionar servicios de DPP, incluyendo el mantenimiento de una copia de seguridad del DPP.

- **Autoridad pública (Public Authority):** Se refiere a las partes que cumplen con los deberes que les asigna la ley, como las autoridades aduaneras o las autoridades de vigilancia del mercado.

- **Agencia de credenciales (Credentials Agency):** Una persona jurídica que proporciona credenciales a las partes, las cuales pueden ser utilizadas para hacer y verificar una variedad de reclamaciones en el DPP.

- **Actor de la cadena de suministro (Supply Chain Actor):** Una persona jurídica que realiza una actividad en la cadena de valor de un producto hasta el punto en que el producto llega al cliente.

La claridad en la definición de estos roles es vital para garantizar la eficiencia, la responsabilidad y la confianza en la compartición de datos dentro del sistema DPP. BAIDATA, como actor facilitador, busca precisamente conectar a estos diferentes roles, promoviendo el entendimiento mutuo y la colaboración para maximizar el valor de la economía del dato.

1.4. Estructura del documento: navegando los fundamentos del DPP

Para facilitar una comprensión clara y progresiva de la Arquitectura de Referencia del Pasaporte Digital de Producto (DPP), este documento se ha estructurado cuidadosamente en varias secciones clave. Su diseño busca guiarle desde los conceptos más generales hasta los detalles esenciales, permitiéndole asimilar el "plano" del DPP de forma eficiente.

A lo largo de las siguientes secciones, exploraremos:

- **Bloques de construcción:** Esta sección fundamental se adentra en los diferentes actores y roles clave que interactúan en el ecosistema del DPP. Se detallan sus responsabilidades y cómo cada uno contribuye al flujo de información y a la operatividad del sistema, desde los operadores económicos responsables hasta las autoridades públicas y los proveedores de servicios.

- **Recomendaciones arquitectónicas clave:** Aquí se abordarán las directrices fundamentales y las mejores prácticas para el diseño y la implementación de la arquitectura del DPP. Se cubrirán aspectos críticos como la interoperabilidad, la gestión de la identidad y el acceso, la integridad de los datos y su visualización.

- **Riesgos y mitigaciones:** Esta parte crucial identificará los posibles desafíos y riesgos asociados con el despliegue y la operación del DPP, junto con estrategias y enfoques para mitigarlos, asegurando un camino más robusto y seguro hacia su implementación.

- **Apéndices:** El documento concluirá con apéndices que ofrecen información adicional y detallada, proporcionando un soporte complementario para una comprensión más profunda de ciertos aspectos técnicos y normativos del DPP.

Esta estructura está diseñada para que, sin necesidad de ser un experto técnico, usted pueda comprender los fundamentos de la Arquitectura de Referencia del DPP y su implicación para la economía del dato.

2. BLOQUES DE CONSTRUCCIÓN

Los "Bloques de construcción" de la arquitectura del Pasaporte Digital de Producto (DPP) se presentan en este documento con un **enfoque funcional**.

Los autores han optado por esta metodología para que la arquitectura sea más **accesible y práctica**, relacionando directamente los componentes técnicos con las capacidades que permiten a cada actor cumplir sus funciones dentro del ecosistema.

A continuación, se detallan estos bloques de construcción clave, explicando su interacción y relevancia a través de la lente de los diferentes actores del ecosistema del DPP.

2.1. Operador económico responsable (rEO)

El **Operador Económico Responsable (rEO)** es un actor central en la creación y gestión del Pasaporte Digital de Producto (DPP), siendo el principal responsable de asegurar la información y funcionalidad de estos. Su rol implica una interacción directa o indirecta con una serie de bloques de construcción esenciales y opcionales, permitiéndole cumplir sus responsabilidades a lo largo del ciclo de vida del producto. El documento de referencia señala que esta agrupación por rol es indicativa y puede evolucionar con el tiempo, dando lugar a diversas combinaciones de bloques según las necesidades.

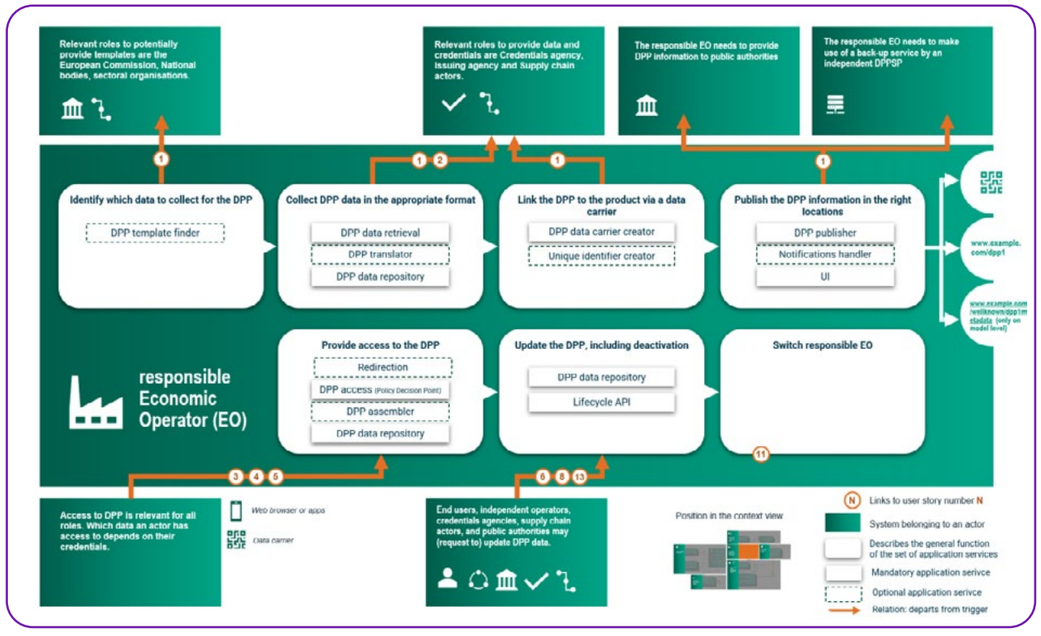

Figura 3. Bloques de construcción desde la perspectiva del REO

A continuación, se describen los bloques de construcción clave para el rEO:

- **DPP Template Finder (Buscador de Plantillas DPP) (Opcional):** Este servicio es fundamental para el rEO al permitirle identificar y seleccionar modelos de datos o plantillas de DPP relevantes para un tipo de producto específico, incluyendo tanto datos obligatorios como voluntarios. Funciona recibiendo como entrada el tipo de producto y, opcionalmente, el caso de uso, y proporcionando como salida una plantilla adecuada y metadatos sobre las plantillas disponibles. Estas plantillas pueden proceder de diversas fuentes, como autoridades públicas o entidades sectoriales y empresariales, y se recomienda la agregación y búsqueda estandarizada para facilitar su descubrimiento. Las plantillas pueden definirse usando formatos como JSON Schema y SHACL, y se sugiere estandarizar el formato de intercambio a JSON-LD.

- **DPP Data Retrieval (Recuperación de Datos DPP) (Opcional):** Para completar un DPP, el rEO a menudo necesita recopilar información relevante. Este bloque opcional facilita la recolección de datos provenientes de diversos actores de la cadena de suministro, utilizando diferentes protocolos para consolidar la información necesaria para el Pasaporte. Requiere detalles de conexión a fuentes de datos y credenciales de acceso como entrada, y produce el conjunto de datos recopilados para crear el DPP. Si los datos no están en un formato legible por máquina, puede necesitar una conversión manual o asistida. Se destacan los acuerdos en la cadena de suministro para la recopilación y el intercambio de información como una recomendación clave.

- **DPP Translator (Traductor DPP) (Opcional):** Dada la heterogeneidad de fuentes y formatos, el rEO puede requerir este servicio opcional para convertir los datos del DPP entre distintos modelos y niveles de granularidad, ofreciendo capacidades de mapeo y conversión de formatos. Su entrada son los datos del DPP, junto con información sobre el modelo, formato (como JSON-LD, CSV, AAS) e idioma de destino. Como salida, proporciona los datos del DPP convertidos al modelo, granularidad, idioma y formato deseados. Este servicio es útil tanto al acceder a un DPP en un formato personalizado como al recibir datos de actores de la cadena de suministro. La recomendación principal es definir reglas de mapeo y utilizar un motor que realice la conversión automáticamente.

- **DPP Data Repository (Repositorio de Datos DPP):** Este bloque constituye el sistema de almacenamiento central donde se albergan los datos reales del DPP asociados a un Identificador Único de Producto (UPI). Actúa como un punto centralizado (lógico, aunque puede ser descentralizado físicamente) con interfaces para almacenar nuevos datos y recuperar los existentes. Para la recuperación, toma un UPI y devuelve los datos; para el almacenamiento, acepta los datos, metadatos y eventos asociados a un UPI. Su implementación puede ser variada, pero se recomienda una API REST que use JSON-LD para interoperabilidad. Es crucial que el repositorio asegure la inmutabilidad de los registros de DPP y soporte firmas/sellos digitales para garantizar la integridad de los datos.

- **Unique Identifier Creator (Creador de Identificador Único):** Es esencial que el rEO pueda generar identificadores únicos que vinculen el producto físico con su representación digital, garantizando que sean únicos y armonizables en la UE. Este bloque de construcción permite la creación de identificadores clave como el Identificador Único de Producto (UPI), el Identificador Único de Instalación (UFI) y el Identificador Único de Operador (UOI). No requiere entrada específica, y su salida es el identificador único generado. Se consideran diversos estándares y sistemas para la generación de estos identificadores, y se recomienda usar operadores que cumplan con los estándares JTC24 para garantizar la conformidad con los requisitos del ESPR.

- **DPP Data Carrier Creator (Creador de Soporte de Datos DPP):** El rEO es responsable de la creación del soporte de datos (ej. código QR o código de barras) que contendrá el identificador único del producto o un enlace web para acceder al DPP. Este bloque genera dicho portador, requiriendo el identificador o enlace y el formato deseado como entrada, y produciendo el portador de datos codificado como salida. Se prefiere un portador que pueda ser leído por smartphones estándar, aunque otros son posibles para escenarios B2B específicos. Se deben considerar estándares relevantes y es importante pensar en la accesibilidad para usuarios vulnerables. Se recomienda establecer un símbolo universal para el DPP en el producto.

- **DPP Publisher (Publicador DPP):** Este bloque permite al rEO hacer que los datos del DPP, incluidas sus actualizaciones, estén disponibles para las partes interesadas a través de un endpoint dedicado. A diferencia del repositorio, se centra en la disponibilidad externa. Requiere el UPI (para registro) y una URL accesible como entrada, así como parámetros para la creación de índices o enlaces a actualizaciones, y proporciona una URL accesible que permite recuperar el DPP. Para mejorar la detectabilidad, se recomienda encarecidamente que los Operadores Económicos responsables alojen metadatos que especifiquen la ubicación de los datos a nivel de modelo de producto bajo /.well-known/dpp/....

- **Notifications Handler (Gestor de Notificaciones) (Opcional):** Este servicio opcional facilita al rEO el envío de alertas y comunicaciones sobre eventos relacionados con el DPP a las partes interesadas, como notificar a un EO de una actualización o cambio de estado de un producto. Toma como entrada ubicaciones de repositorios o información de conexión y tipos de eventos a notificar, y su salida es una notificación enviada al actor apropiado con los datos del evento relevante. Las notificaciones pueden ser push, in-app o por correo electrónico, y pueden distribuirse mediante mecanismos como message brokers o webhooks.

- **UI (Interfaz de Usuario):** Aunque la implementación de la interfaz de usuario pueda recaer en terceros, el rEO se beneficia de este bloque para asegurar que los usuarios finales y otros actores puedan visualizar los DPP de manera clara y accesible. Proporciona la representación visual de los datos del DPP para el usuario final, requiriendo los datos del DPP como entrada y produciendo una representación visual como salida. Las recomendaciones clave incluyen la creación de un conjunto universal de símbolos para datos clave del DPP y el desarrollo de plantillas y pautas estandarizadas para la visualización.

- **Redirection (Redirección):** Este bloque es crucial para el rEO, ya que asegura que la URI (identificador de recurso uniforme) de un producto dirija correctamente a los recursos o servicios pertinentes, incluyendo el propio DPP. Traduce el URI de un producto a uno o más URIs “activos” que permiten el acceso a recursos o servicios asociados, y facilita la modificación posterior del conjunto de recursos accesibles. Toma el URI de un producto como entrada y produce URIs resueltas como salida. Puede funcionar como un proxy o usar redirecciones HTTP estándar. Es vital que el servicio siga operativo incluso si el EO responsable cesa sus actividades. Se recomienda utilizar credenciales verificables eIDAS 2.0 para la gestión de roles y asegurar que las credenciales sean emitidas por cuerpos de confianza.

- **Access Control Policy Decision Point (Punto de Decisión de Política de Control de Acceso):** Fundamental para el rEO, este bloque evalúa las solicitudes de acceso a los datos y funcionalidades del DPP frente a políticas de autorización predefinidas. Concede o revoca el acceso basándose en las credenciales proporcionadas, asegurando así la seguridad y la privacidad de la información del DPP.

- **DPP Assembler (Ensamblador DPP):** Cuando se solicita un DPP, este bloque se encarga de reunir toda la información necesaria para construirlo. Puede recuperar un DPP completo

preensamblado o combinar datos de múltiples fuentes, incluyendo repositorios del rEO y de Operadores Independientes. Toma un ID de producto único como entrada, con opciones para especificar formato, subconjunto de datos, credenciales o fecha histórica. La salida es el dato del DPP formateado según lo requerido, o como un documento HTML por defecto, posiblemente incluyendo datos restringidos si se proporcionan credenciales. Se discuten opciones de implementación como recuperar de una fuente única o múltiples fuentes, y se destaca la necesidad de capacidades de mapeo de datos.

- **Lifecycle API (API de Ciclo de Vida):** El rEO interactúa con este conjunto de interfaces programáticas estandarizadas para gestionar las operaciones del ciclo de vida del DPP, incluyendo CREAR, ACTUALIZAR, ACCEDER, ELIMINAR y RESPALDO/TRANSFERENCIA. Se espera que esta API sea definida por el estándar JTC24. Las operaciones de "actualización" y "eliminación" deben ser lógicas (añadir nuevas entradas o marcar estado) respetando la inmutabilidad. Las entradas/salidas varían según la operación. Se recomienda que los endpoints para operaciones de escritura acepten parámetros para verificación de autenticidad y que el formato de carga útil sea JSON-LD. La adopción de esta API estándar es una recomendación clave.

2.2. Autoridades públicas

Las **Autoridades Públicas** desempeñan un rol fundamental en el ecosistema del Pasaporte Digital de Producto (DPP), siendo responsables de la supervisión, cumplimiento y aplicación de las regulaciones. Su interacción con el sistema DPP se basa en la necesidad de acceder a información clave para verificar la conformidad de los productos y los datos asociados. Los siguientes bloques de construcción son esenciales desde su perspectiva para interactuar con el sistema DPP:

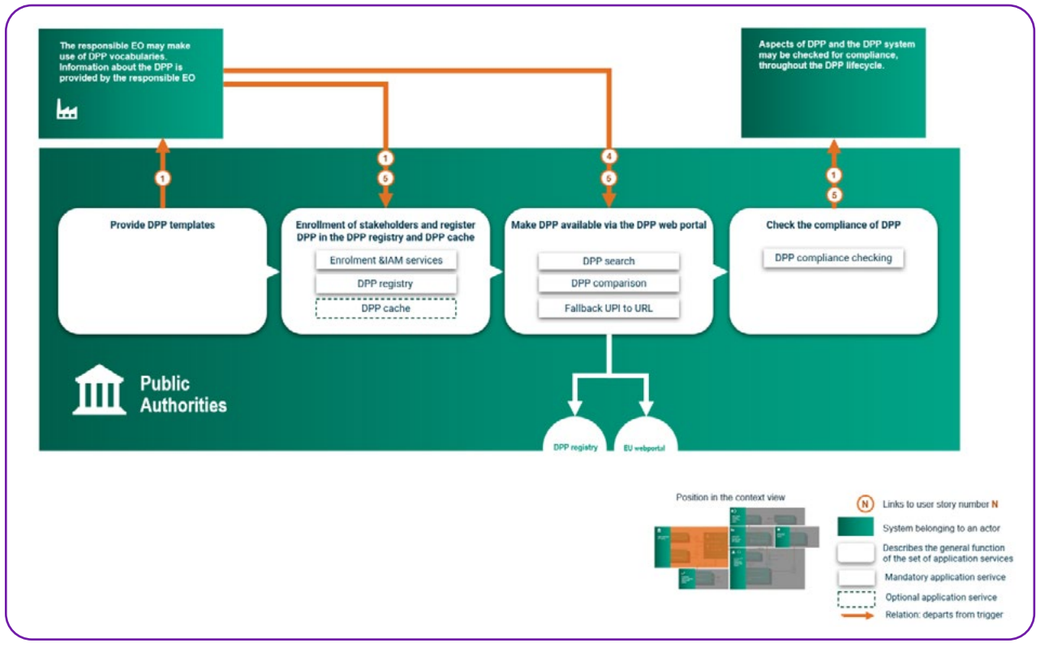

Figura 4. Bloques de construcción desde la perspectiva de las Autoridades Públicas

- **(EU) DPP Registry (Registro DPP de la UE):** Este es un bloque central para las Autoridades Públicas, ya que les permite acceder a un registro comprensivo de todos los DPPs emitidos en el mercado común. Contiene información mínima esencial como el ID del Producto, ID del rEO, ID de la Instalación, la ubicación del DPP y su estado actual de ciclo de vida. Este servicio, proporcionado por la Comisión Europea (EC), es crucial para las funciones de control y supervisión. Verifica los identificadores antes de aceptar un DPP y proporciona una confirmación de registro exitoso o fallo. Si se implementa el servicio de redirección de fallback de la UE o la búsqueda centralizada, la información relevante también debería registrarse aquí.

- **DPP Compliance Checking (Comprobación de Cumplimiento DPP):** Este bloque habilita a las Autoridades Públicas para verificar que un conjunto específico de datos del DPP cumple con las normativas y regulaciones aplicables. Compara un conjunto de datos de DPP con las reglas, regulaciones y acuerdos apropiados. Toma datos de DPP en formato JSON-LD y, opcionalmente, la identificación de la plantilla o una plantilla SHACL para la validación. La salida es el resultado de la validación, incluyendo información sobre los fallos si los hay. La validación debe realizarse según el nivel de granularidad y los actos delegados correspondientes, e implementarse posiblemente como un aplicador de plantillas SHACL.

- **DPP Search (Búsqueda DPP):** La funcionalidad de búsqueda es vital para las Autoridades Públicas, permitiéndoles buscar datos de DPP según criterios de búsqueda. Estos criterios pueden ser a nivel de modelo (marca, nombre) o a nivel completo (tipo de producto, operador económico, UPI). El servicio puede devolver datos de DPP a nivel de modelo o el DPP completo. Es una funcionalidad central del Portal Web de la CE. La complejidad depende de los criterios permitidos; si se permiten búsquedas basadas en campos descentralizados, se necesita una estrategia eficiente, como crear un índice de búsqueda centralizado para datos clave.

- **Fallback Product UPI to URL (Redirección de UPI de Producto a URL de Fallback):** Este bloque es un servicio fundamental diseñado para determinar automáticamente la ubicación de un DPP a partir de un Identificador Único de Producto (UPI) o un enlace web basado en él. Este servicio es proporcionado por la Comisión Europea o entidades delegadas y actúa como un mecanismo de fallback (mecanismo de respaldo) neutral respecto al proveedor. Su entrada es un UPI o enlace web, y su salida es uno o más enlaces web que permiten el acceso al DPP. Debe cumplir con los estándares relevantes y asegurar la disponibilidad a largo plazo, incluso en casos de insolvencia del rEO o DPPSP.

- **DPP Comparison (Comparación de DPP):** Este bloque de construcción permite comparar datos entre al menos dos (o potencialmente múltiples) Pasaportes Digitales de Producto (DPP) basándose en criterios relevantes. Es particularmente útil para los consumidores antes de comprar un producto y será habilitado por el Portal Web de la CE. Recibe un conjunto de datos de múltiples DPP y opciones de comparación como entrada. Proporciona una comparación visual y personalizable de los datos de los DPP como salida.

- **Enrolment & IAM Services (Servicios de Registro y Gestión de Identidad y Acceso - IAM):** Aunque no es un bloque de interacción directa con el DPP en sí mismo, este servicio es esencial para las Autoridades Públicas al facilitar la asignación de un identificador, una identidad y roles a un Operador Económico. Este paso es necesario para la emisión de credenciales y para asegurar que los Operadores Económicos tengan un identificador válido requerido para el registro del DPP. Requiere información personal y de la empresa del EO, así como el rol que desea desempeñar. La salida es un mensaje que comunica el resultado de la operación y el identificador y/o roles asignados. Se recomienda que la CE implemente este servicio y que se base en credenciales verificables (VCs), idealmente eIDAS 2.0, emitidas por cuerpos de

confianza. Es crucial que el sistema soporte control de acceso basado en roles genéricos.

- **DPP Cache (Caché DPP):** Este bloque de construcción consiste en un caché de datos del Pasaporte Digital de Producto (DPP) o de algunos de sus elementos. Dada la naturaleza potencialmente descentralizada del DPP, su función es especialmente relevante para acelerar la búsqueda y recuperación de información, al permitir la centralización temporal de datos relevantes y, con ello, optimizar el rendimiento general del sistema.

2.3. Proveedor de servicios de DPP (DPPSP)

El **Proveedor de servicios de DPP (DPPSP)** es una entidad esencial en el ecosistema del Pasaporte Digital de Producto, cuya función principal es asegurar la gestión, disponibilidad y transferencia segura de los datos del DPP. Sus servicios son cruciales para la integridad y la continuidad a largo plazo de la información del Pasaporte Digital.

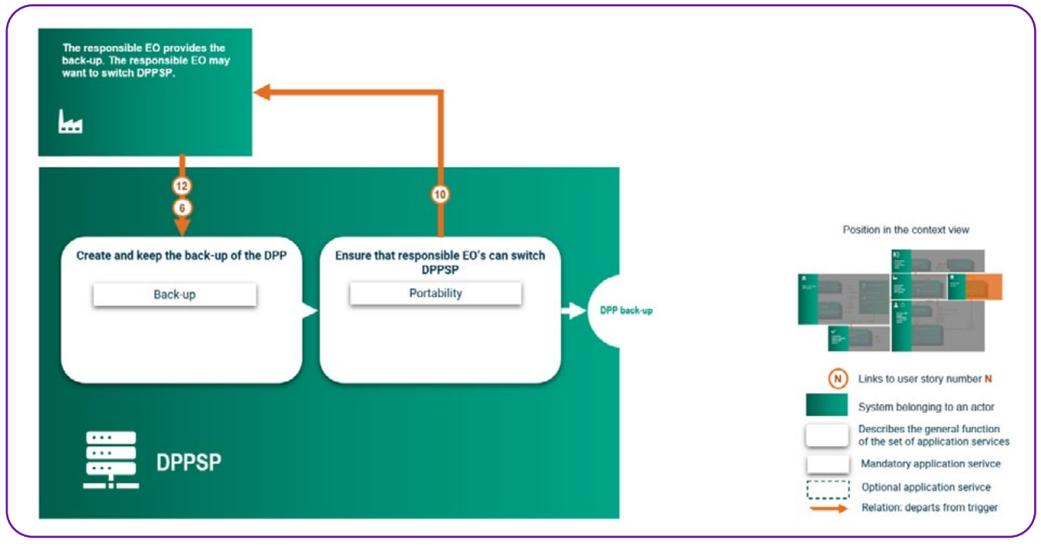

Figura 5.Bloques de construcción desde la perspectiva de los proveedores de servicios de DPP

Los bloques de construcción clave que el documento asocia a este rol son dos:

- **BACK-UP (Copia de seguridad):** Este bloque se dedica a almacenar datos de DPP de forma independiente del Operador Económico responsable. Debe almacenar todos los datos obligatorios del DPP y aceptar actualizaciones, pudiendo también almacenar datos adicionales de forma opcional. Recibe datos y actualizaciones del DPP, así como restricciones de acceso. Proporciona confirmación de almacenamiento exitoso y la ubicación del respaldo, y puede devolver los datos del DPP. Es vital que el proveedor de respaldo almacene todos los datos, incluidos los opcionales, y aplique las mismas reglas de control de acceso que el rEO principal. El formato de intercambio JSON-LD y la adopción de la API de Ciclo de Vida son recomendaciones relevantes.

- **PORTABILITY (Portabilidad del DPP):** Este bloque permite transferir datos de DPP, incluyendo respaldos y enlaces a actualizaciones, entre entidades. Su propósito principal es la transferencia de datos para respaldo y el cambio de proveedor de servicios de DPP. Toma datos obligatorios y opcionales del DPP, así como restricciones de acceso. Proporciona confirmación de transferencia exitosa y la ubicación de los datos transferidos. Se recomienda garantizar la redirección UPI a URI y adoptar la API de Ciclo de Vida estándar.

2.4. Usuario final y Operador independiente (End User and Independent Operator)

Los usuarios finales (consumidores, empresas) y los operadores independientes (como reparadores, recicladores o mercados de segunda mano) son actores cruciales en el ciclo de vida del producto y el ecosistema del DPP. Su interacción con el DPP se centra principalmente en el acceso, la lectura y la utilización de la información del producto para diversas finalidades, desde la toma de decisiones de compra hasta la gestión de residuos o la prestación de servicios.

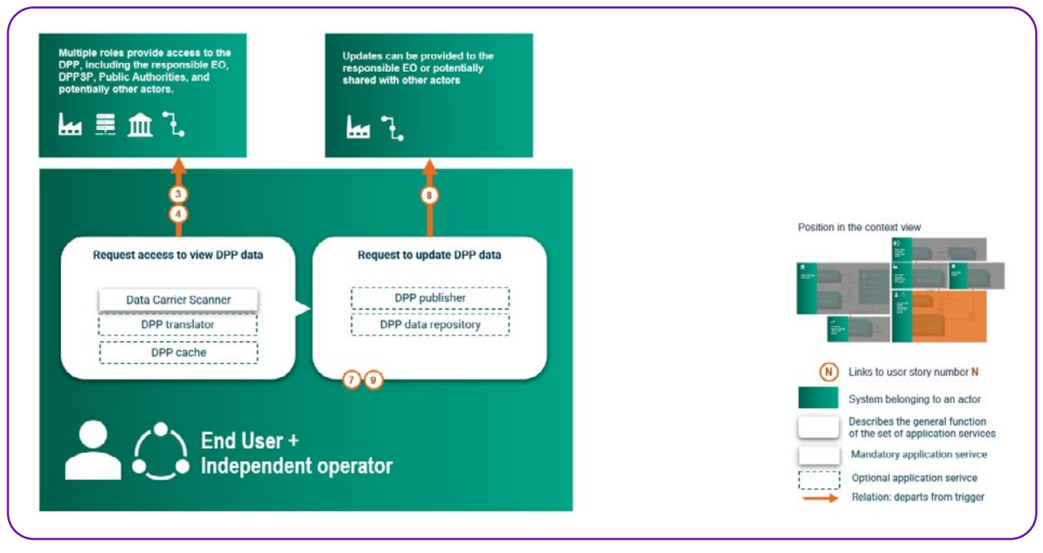

Figura 6.Bloques de construcción desde la perspectiva de los usuarios finales y los operadores independientes

Los bloques de construcción clave que el documento asocia a estos roles son:

- **Data Carrier Scanner (Escáner de portador de datos):** Este bloque es utilizado principalmente por usuarios finales y operadores independientes para leer la información codificada en el portador de datos físico de un producto. Su función es procesar esta información para

obtener el identificador único del producto o un enlace web para acceder al DPP. Toma el portador de datos del producto como entrada y proporciona el UPI o enlace web decodificado y resuelto, junto con cualquier dato adicional, como salida. Idealmente, la cámara de un smartphone debería ser suficiente para leer portadores como códigos QR que contengan una URL directamente resoluble, aunque podrían ser necesarias aplicaciones específicas o dispositivos ad-hoc para casos más complejos. Se recomienda crear un portador de datos específico para uso online y pre-compra.

- **DPP translator (Traductor DPP):** Para una descripción detallada de este bloque, consulte la Sección 2.1 Operador económico responsable (rEO).
- **DPP Cache (Caché DPP):** Para una descripción detallada de este bloque, consulte la Sección 2.2 Autoridades públicas.
- **DPP publisher (Publicador DPP):** Para una descripción detallada de este bloque, consulte la Sección 2.1 Operador económico responsable (rEO).
- **DPP data repository (Repositorio de Datos DPP):** Para una descripción detallada de este bloque, consulte la Sección 2.1 Operador económico responsable (rEO).

2.5. Agencia de credenciales y agencia emisora (Credentials Agency and Issuing Agency)

La Agencia de Credenciales y la Agencia Emisora son roles esenciales en el ecosistema del DPP, responsables de establecer y mantener la confianza y la seguridad a través de la gestión de identidades y la emisión de credenciales. Aseguran que solo los actores autorizados puedan acceder y operar dentro del sistema DPP, garantizando la integridad de los datos y las operaciones.

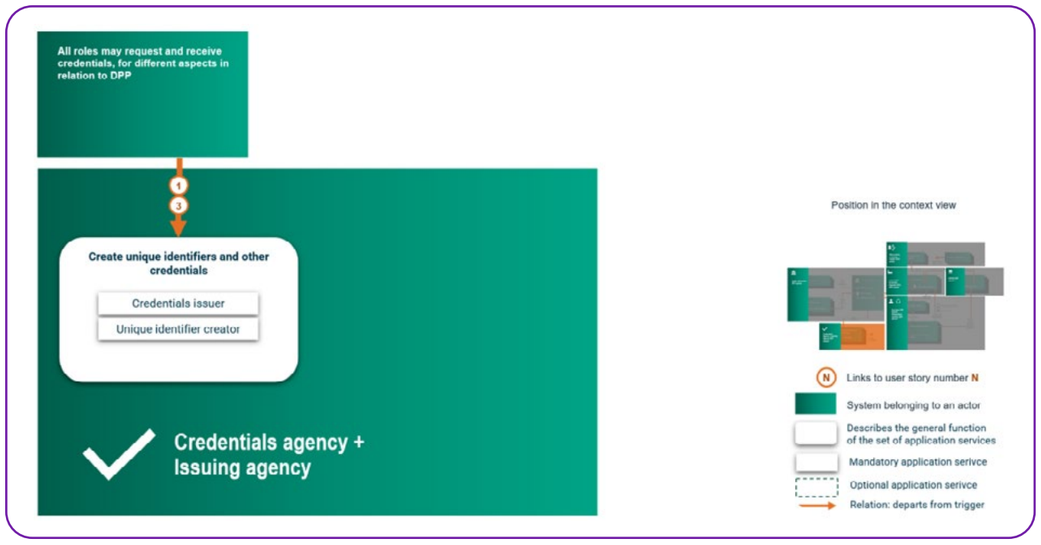

Figura 7.Bloques de construcción desde la perspectiva de la agencia de credenciales y la agencia emisora

Los bloques de construcción clave asociados a este rol son:

- **Credential Issuer (Emisor de Credenciales):** Este servicio fundamental evalúa las solicitudes y asigna credenciales y roles específicos a los actores autorizados dentro del sistema DPP, definiendo así su alcance de acceso. Recibe como entrada la prueba de identidad del actor solicitante y emite las credenciales en el formato adecuado (como SD-JWT) o un mensaje de rechazo. Se recomienda encarecidamente el uso de Verifiable Credentials (VCs), preferiblemente compatibles con eIDAS 2.0 y emitidas por cuerpos de confianza (idealmente gubernamentales o con mandato gubernamental), para la gestión de identidad y roles. Esta función está estrechamente ligada al control de acceso basado en roles (RBAC), y el emisor debe mantener un registro de las credenciales revocadas o expiradas.
- **Unique Identifier Creator (Creador de Identificador Único):** Para una descripción detallada de este bloque, consulte la Sección 2.1 Operador económico responsable (rEO).

2.6. Otros actores, incluidos los actores de la cadena de suministro (Other Actors, Including Supply Chain Actors)

Este rol abarca a una variedad de actores, desde proveedores de materiales y componentes hasta distribuidores, minoristas y otros participantes en la cadena de suministro, así como entidades que ofrecen servicios de valor añadido. Su interacción con el DPP se centra en el intercambio de información, la contribución de datos y el uso de la información del pasaporte para optimizar procesos y ofrecer nuevos servicios a lo largo de la vida del producto.

Figura 8.Bloques de construcción desde la perspectiva de otros actores

Los bloques de construcción clave que el documento asocia a este rol son:

- **DPP Analytics (Analíticas del DPP):** Este bloque opcional utiliza datos de DPP para proporcionar información y análisis específicos. Puede ser útil tanto para los Operadores Económicos Responsables (rEO) para obtener información sobre el ciclo de vida del producto, como para las autoridades públicas para realizar vigilancia del mercado y verificaciones de cumplimiento. Toma los datos del DPP y las especificaciones del análisis requerido como entrada, y su salida es la información requerida o los resultados del análisis. Dado que un DPP se basa en ontologías, un servicio de analíticas podría tomar la forma de un razonador semántico. Se recomienda estandarizar el formato de intercambio a JSON-LD y alinearse con las APIs existentes para servicios de valor añadido.
- **DPP Comparisons (Comparación de DPP):** Para una descripción detallada de este bloque, consulte la Sección 2.2 Autoridades públicas.
- **DPP Associated Data Registers (Registros de Datos Asociados al DPP):** Este bloque opcional almacena datos voluntarios para complementar un DPP. Esto incluye información no obligatoria no almacenada por el rEO, como reseñas, datos de ONG o datos de reparación no requeridos legalmente. Toma datos adicionales de DPP y el UPI/URL del DPP como entrada, y proporciona información registrada asociada al DPP como salida. Se recomienda alinearse con las APIs existentes para servicios de valor añadido.

3. RECOMENDACIONES ARQUITECTÓNICAS CLAVE

Las recomendaciones arquitectónicas para el Pasaporte Digital de Producto (DPP) se agrupan en seis áreas principales, con el objetivo de abordar los desafíos inherentes a la implementación de un sistema DPP a nivel de ecosistema y asegurar su interoperabilidad, seguridad, fiabilidad y facilidad de uso para todos los actores involucrados.

3.1. Interoperabilidad

La interoperabilidad es un pilar fundamental para el éxito del ecosistema del Pasaporte Digital de Producto, ya que garantiza que los diversos componentes y sistemas DPP, desarrollados por diferentes actores, puedan comunicarse e intercambiar información de manera fluida y comprensible. Esta capacidad es esencial para permitir que la información del DPP sea utilizada eficazmente a lo largo de toda la cadena de valor y por múltiples partes interesadas, desde los Operadores Económicos Responsables hasta las autoridades públicas y los consumidores. Las recomendaciones en esta área buscan establecer un 'idioma digital' común y mecanismos estandarizados que faciliten el flujo de datos.

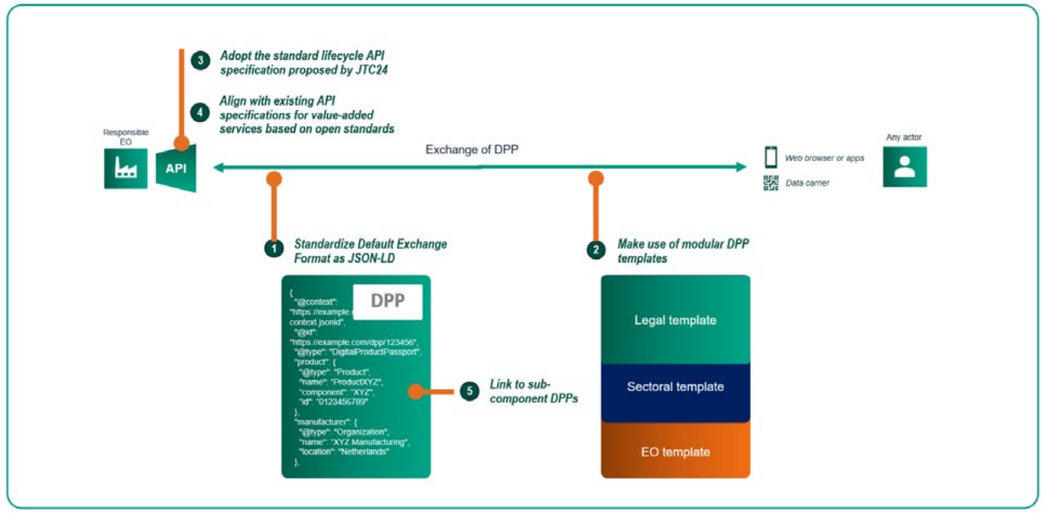

Figura 9. Recomendaciones de interoperabilidad

Las recomendaciones clave en el área de interoperabilidad son:

1. Estandarizar el formato de intercambio predeterminado a JSON-LD (p. 32)
2. Utilizar plantillas DPP modulares (p. 33)
3. Adoptar la especificación de la API de ciclo de vida a la propuesta por JTC24 (p. 34)
4. Alinear con las especificaciones de API existentes para servicios de valor añadido (p. 35)
5. Enlazar a los DPPs de componentes de producto (p. 36)

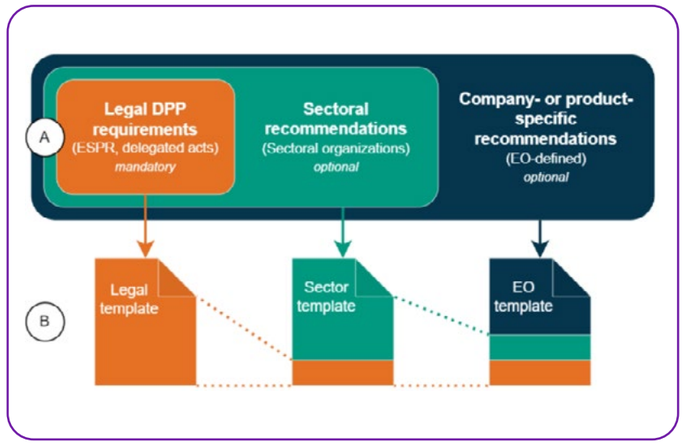

Figura 10. Estructura de plantillas anidadas de CIRPASS

3.2. Gestión de identidad y acceso

La gestión de identidad y acceso es crítica para la seguridad y la confianza en el sistema DPP, pues define con precisión quién tiene permiso para acceder y manipular la información. Esta área aborda cómo se verifica la identidad de los actores que interactúan con el DPP y qué nivel de granularidad se aplica a sus derechos de acceso. Implementar mecanismos robustos en esta área es vital para proteger los datos sensibles y asegurar el cumplimiento de las normativas de privacidad y seguridad, estableciendo una base fiable sobre quién está interactuando con el sistema.

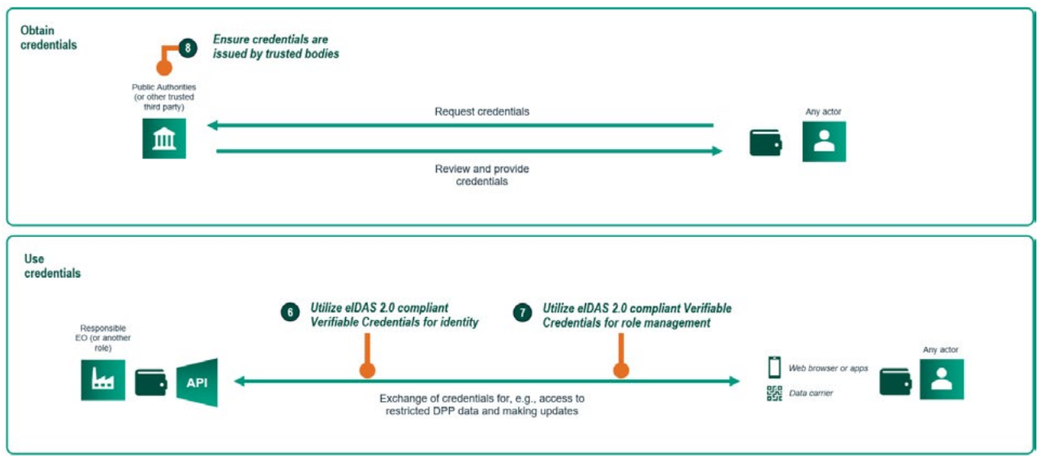

Figura 11. Recomendaciones de gestión de identidad y acceso

Las recomendaciones clave en el área de gestión de identidad y acceso son:

6. Utilizar Credenciales Verificables emitidas centralmente para la identidad (p. 37)
7. Utilizar control de acceso basado en roles genéricos (p. 39)
8. Asegurar que las credenciales sean emitidas por entidades de confianza (p. 41)

3.3. Integridad del DPP

La integridad del DPP es esencial para garantizar la fiabilidad y la validez de la información a lo largo de todo el ciclo de vida del producto. Esta área se enfoca en la implementación de mecanismos robustos que aseguren que los datos contenidos en el DPP sean auténticos, precisos y que no hayan sido manipulados de forma indebida. Las recomendaciones aquí buscan establecer un marco de confianza para todas las entradas y actualizaciones del DPP, permitiendo a los usuarios confiar plenamente en la información que consumen, incluso a lo largo del tiempo y tras múltiples interacciones.

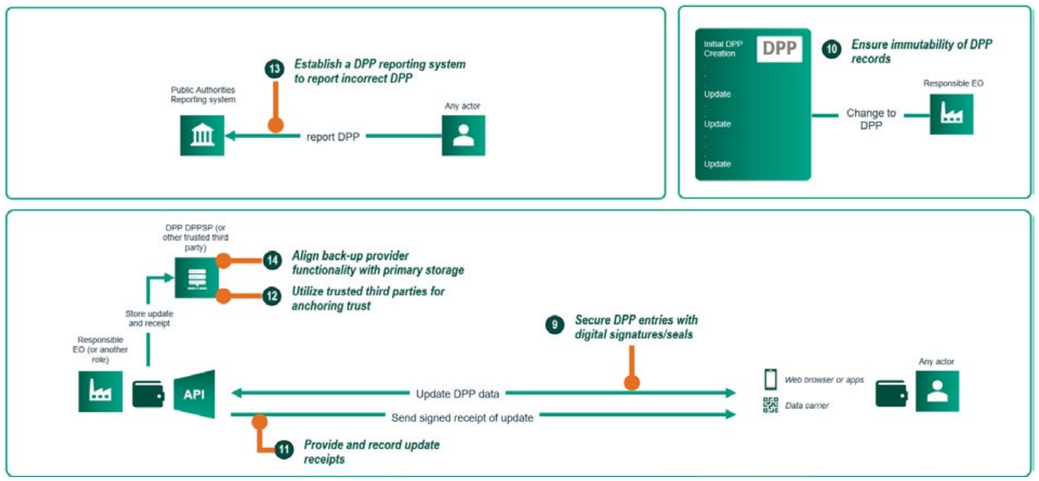

Figura 12. Recomendaciones de gestión de integridad del DPP

Las recomendaciones clave para asegurar la integridad del DPP son:

9. Proteger las entradas del DPP con firmas/sellos digitales (p. 43)
10. Asegurar la inmutabilidad de los registros del DPP (p. 44)
11. Proporcionar y registrar recibos de actualización (p. 44)
12. Utilizar terceros de confianza para anclar la confianza (p. 45)
13. Establecer un sistema de notificación de DPPs para reportar DPPs incorrectos (p. 45)
14. Alinear la funcionalidad del proveedor de respaldo con el almacenamiento principal (p. 46)

3.4. Acceso al DPP

El acceso eficiente al DPP es fundamental para su utilidad por parte de todos los actores del ecosistema. Esta sección describe los mecanismos y servicios necesarios para que los usuarios puedan encontrar, localizar y recuperar los datos de un DPP de manera sencilla y fiable, independientemente de su ubicación o del estado operativo del Operador Económico Responsable. Las recomendaciones se centran en establecer rutas claras y persistentes para la información, facilitando una experiencia de usuario fluida y garantizando la disponibilidad a largo plazo.

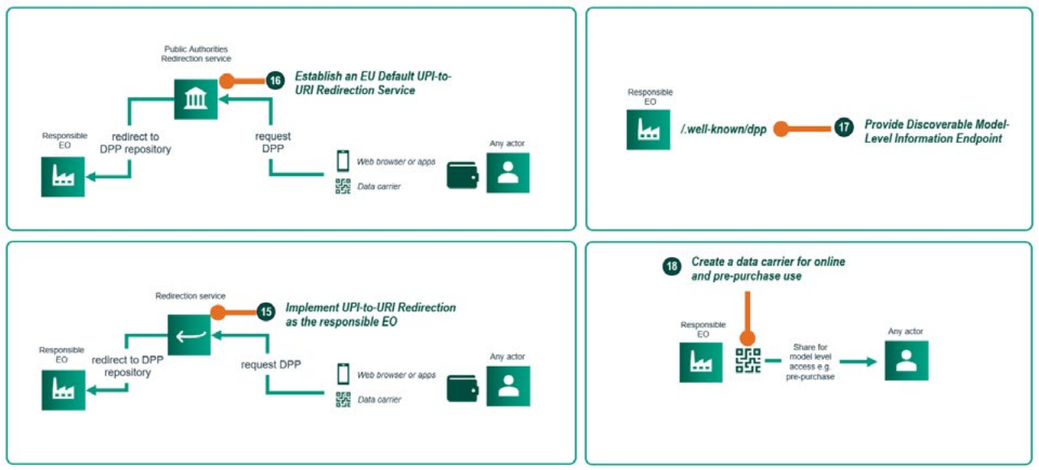

Figura 13. Recomendaciones de gestión de acceso al DPP

Las recomendaciones clave relacionadas con el acceso al DPP son:

15. Asegurar la redirección de UPI a URI como el EO responsable (p. 47)
16. Establecer un servicio de redirección de respaldo de UPI a URI a nivel de la UE (p. 48)
17. Proporcionar un punto final de datos descubrible a nivel de modelo (p. 49)
18. Crear un portador de datos para uso online y de pre-compra (p. 49)

3.5. Gestión de datos

La gestión de datos dentro del ecosistema del DPP se refiere a la organización, el almacenamiento y el manejo eficiente de la vasta cantidad de información generada a lo largo del ciclo de vida del producto. Esta área es crucial para asegurar que los datos estén disponibles cuando se necesiten, que se mantenga un historial completo de actualizaciones y que las búsquedas sean rápidas y precisas. Las recomendaciones aquí buscan optimizar tanto el almacenamiento de datos a nivel de Operador Económico Responsable como la accesibilidad para el ecosistema más amplio, incluyendo el establecimiento de repositorios clave a nivel de la UE.

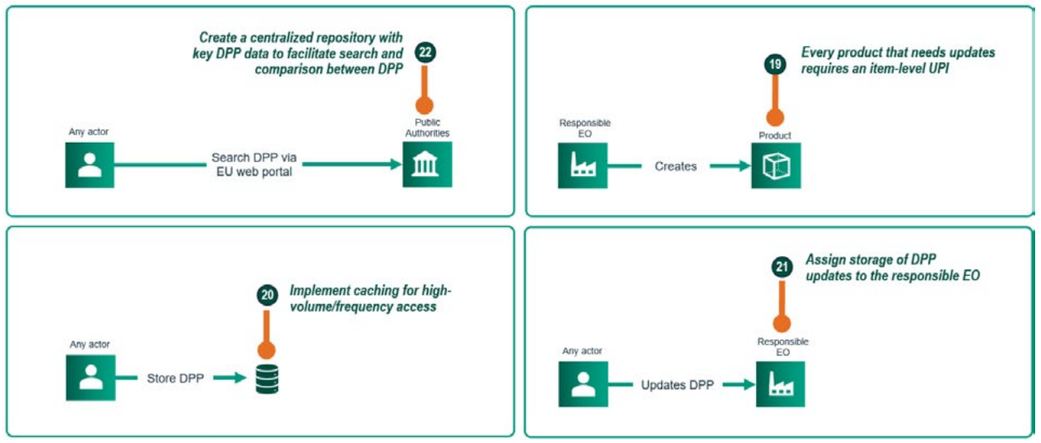

Figura 14. Recomendaciones de gestión de acceso al DPP

Las recomendaciones clave para la gestión de datos son:

19. Cada producto que necesita actualizaciones requiere un UPI a nivel de ítem (p. 51)
20. Implementar caché para acceso de alto volumen/frecuencia (p. 52)
21. Asignar el almacenamiento de las actualizaciones del DPP al EO responsable (p. 52)
22. Establecer un Repositorio de la UE con datos clave del DPP para la búsqueda (p. 53)

3.6. Visualización

La visualización efectiva es clave para la usabilidad y la comprensión del DPP por parte de los usuarios finales y otros actores, permitiendo que la información compleja se transmita de manera clara y concisa. Esta área se centra en cómo se presenta la información del DPP de manera clara, concisa y accesible, superando las barreras del idioma y la complejidad de los datos técnicos. Las recomendaciones buscan estandarizar la forma en que los usuarios interactúan con el DPP, garantizando una experiencia coherente y permitiendo una rápida captación de la información más relevante para la toma de decisiones o la realización de tareas.

Las recomendaciones clave para la visualización de la información del DPP son:

23. Establecer un símbolo universal del DPP para colocar en el producto (p. 54)
24. Crear un conjunto de símbolos universales para datos clave del DPP (p. 54)
25. Desarrollar plantillas y directrices estandarizadas para la visualización del DPP (p. 55)

Estas recomendaciones buscan crear un ecosistema DPP que sea interoperable, seguro, confiable y fácil de usar para todos los actores, desde los operadores económicos hasta los consumidores y las autoridades.

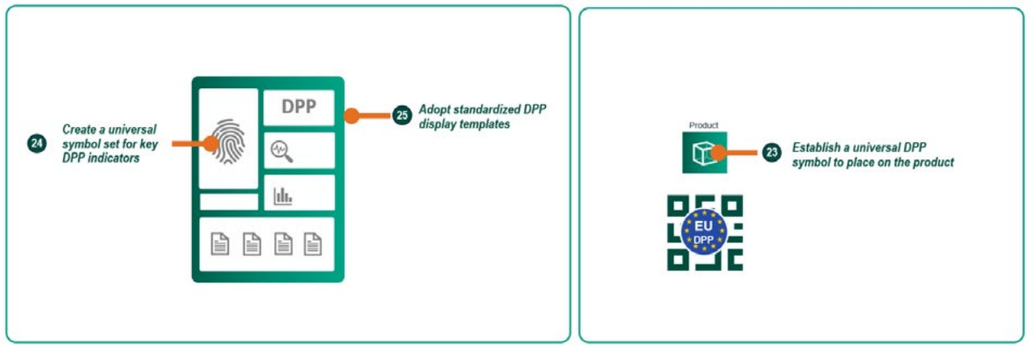

Figura 15. Recomendaciones de gestión de visualización

4. RIESGOS Y MITIGACIONES

La implementación exitosa del sistema del Pasaporte Digital de Producto (DPP) requiere una comprensión profunda y una gestión proactiva de los riesgos potenciales que podrían comprometer su funcionamiento, su integridad o la seguridad de sus usuarios. Esta sección se dedica a identificar y analizar los riesgos técnicos más relevantes para aquellos que diseñan y desarrollan los componentes no centrales de los sistemas DPP compatibles con la normativa ESPR. El objetivo es informar a los desarrolladores sobre las posibles vulnerabilidades para que puedan implementar las mitigaciones necesarias, reconociendo que las decisiones de diseño específicas de cada implementación individual también pueden introducir riesgos adicionales que deben ser considerados. Es fundamental que estos riesgos sean mitigados de manera suficiente para garantizar la fiabilidad y seguridad general del sistema DPP.

4.1. Tipos de Riesgos Técnicos Identificados

El documento identifica y describe varios riesgos técnicos clave, agrupándolos por el momento en que podrían ocurrir en el ciclo de vida del DPP:

- **Riesgos durante la creación y registro del DPP:** Incluyen situaciones como que un operador económico responsable (rEO) falso envíe información inventada al sistema (por ejemplo, al registro de la UE), un rEO que intente realizar un ataque de denegación de servicio (DoS) enviando una cantidad excesiva de DPPs, o la interceptación de información sensible mientras se está transmitiendo para la creación del DPP.

- **Riesgos durante el almacenamiento del DPP y los datos asociados**: Principalmente, se refiere a que el sistema que aloja el DPP sea objetivo de un ciberataque con el fin de robar la información que contiene o comprometer su disponibilidad.

- **Riesgos durante el acceso y la recuperación del DPP por parte de los usuarios o autoridades:** Estos riesgos comprenden la interceptación simple de la información del DPP, la interceptación y modificación de dicha información (ataques de manipulación de datos), o la realización de un ataque “Man-in-the-Middle” donde un actor malicioso se hace pasar tanto por el proveedor del DPP como por el solicitante de datos, interceptando y potencialmente alterando la comunicación.

4.2. Estrategias de Mitigación

Para contrarrestar estos riesgos técnicos, el capítulo menciona posibles mitigaciones que a menudo giran en torno a la implementación de medidas robustas de ciberseguridad. Estas incluyen la utilización de conexiones cifradas y autenticadas para proteger la transmisión de datos, el establecimiento de mecanismos rigurosos de autenticación y autorización para verificar la identidad y los permisos de los actores que interactúan con el sistema, la limitación de la tasa de envío de datos para prevenir ataques de denegación de servicio, y la aplicación de otras medidas generales de ciberseguridad. El conjunto de estas recomendaciones busca fortalecer el sistema contra intentos maliciosos o errores que puedan comprometer la integridad o la confidencialidad de los datos del DPP.

BAIDATA 2025