

## 4. Proyectos Europeos y sistemas de mediación

ACTS (Advanced Communications Technology and Services) es un programa específico del cuarto programa marco de la Comisión Europea en el campo del desarrollo de la investigación tecnológica. Forma parte de una serie de iniciativas que lleva a cabo la Unión Europea con el objetivo de fomentar la investigación y acelerar el proceso de desarrollo de las infraestructuras y servicios avanzados de comunicación.

Dentro del programa ACTS, el Dominio V “Redes y servicios inteligentes” (ACTS Domain V, Intelligence in Services and Networks) pretende contribuir al desarrollo de servicios inteligentes en el ámbito europeo fomentando la creación de técnicas y herramientas que permitan su implantación. Los proyectos del Dominio V de ACTS están relacionados con arquitecturas de servicio, plataformas de servicios, creación de servicios, gestión de comunicaciones, mediación electrónica, movilidad, seguridad y aplicaciones.

En este apartado se realizará una descripción de los proyectos europeos de R&D relacionados con el área de los sistemas intermediarios en el contexto del comercio electrónico. Se han seleccionado aquellos proyectos en los que se presenta una arquitectura abierta de intermediación. A continuación se enumeran los proyectos europeos seleccionados la mayoría de los cuales forman parte del cluster de concertación de ACTS:

- ABS (An Architecture for Information Brokerage Services)
- ABROSE (Agent Based Brokerage Services in Electronic Commerce)
- COBRA (Common Brokerage Architecture)
- GAIA (Generic Architecture for Information Availability)
- OSM (An Open Service Model for Global Information)
- SEMPER (A Security Framework for the Global Electronic Marketplace)

### 4.1 Proyecto ABS

El objetivo del proyecto ABS (Architecture for Information Brokerage System) es el diseño, implementación y validación de un sistema intermediario abierto que permite ofrecer servicios de información en línea (on-line).

En ABS se especificó una arquitectura genérica de un servicio intermediario de información basada en el modelo de referencia de ODP (RM-ODP, Reference Model for Open Distributed Processing), TINA-C y OMG EC-DTF.

El servicio de intermediación no se contempla como un servicio aislado sino que forma parte de una plataforma de mediación comercial. Los servicios de soporte como facturación, pago, entrega y contabilidad no se consideran que forman parte del servicio de intermediación sino de una plataforma de nivel inferior.

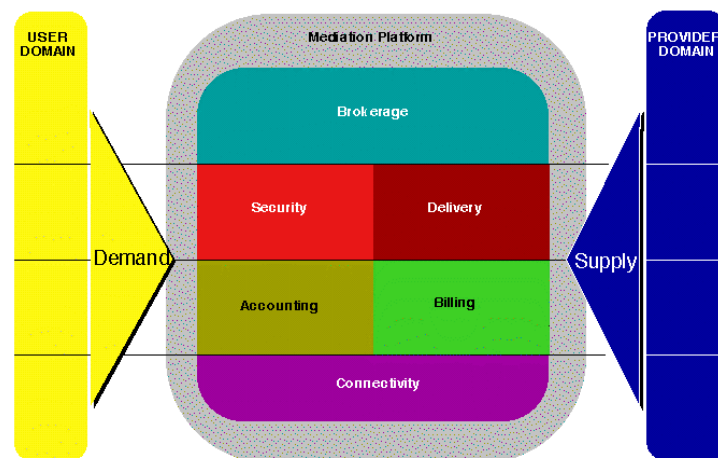


Figura 4-1. ABS: Plataforma de mediación de información

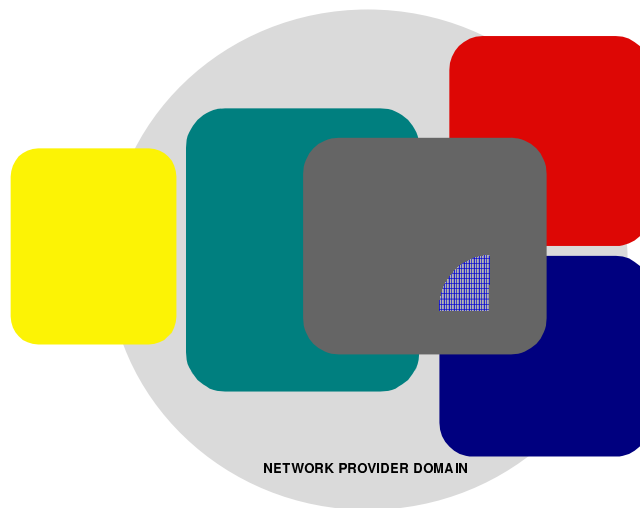
El modelo de ODP propone abordar la descripción de un sistema distribuido mediante cinco puntos de vista o modelos:

- Modelo de negocio
- Modelo de información
- Modelo computacional
- Modelo de ingeniería y tecnológico

#### 4.1.1 Modelo de negocio

El modelo de empresa de ABS define todos los actores, sus dominios, sus relaciones y sus políticas. En el modelo de negocio de ABS se han identificado los siguientes tipos de actores:

- Usuario del servicio de intermediación: Una entidad (máquina, aplicación o persona) que utiliza el servicio de intermediación para satisfacer sus propias necesidades.
- Proveedor servicio de intermediación: Una entidad que ofrece a los usuarios información de servicios o contenidos de otras procedencias.
- Proveedor de servicio: Una entidad proveedora de servicios de telecomunicación, información o aplicaciones. Únicamente son accesibles aquellos servicios disponibles en la red como los sujetos a intermediación (por ejemplo VoD, videoconferencia, etc) o los servicios de soporte (por ejemplo seguridad, pago, certificados, comunicación).
- Proveedor de contenido: Una entidad que ofrece a los usuarios bienes o servicios comerciales negociables a través de servicios de intermediación.
- Minorista: Una entidad que suministra servicios o contenidos a los usuarios (comprados a otras partes) con el acuerdo de los proveedores de servicios y contenidos. El minorista adquiere los objetos o tiene contratos que regulan como tener acceso inmediato a los servicios o contenidos ofrecidos. Se incluyen servicios de intermediación para que los usuarios puedan refinar sus peticiones y localizar los servicios o contenidos más adecuados.
- Proveedor de red: Una entidad que provee al resto de los actores de las funciones de red necesarias.



Una característica del modelo de negocio de ABS es la diferenciación entre los dos actores intermediario y minorista y la introducción de servicios de soporte ofrecidos por actores de otros dominios. La superposición del dominio del minorista con el resto de dominios se debe a que el minorista actúa como un servicio y/o proveedor de servicio utilizando funciones de intermediación.

### 4.1.2 Modelo de información

El modelo de información de ABS presenta un modelo para toda la información almacenada en el sistema y su procesado.

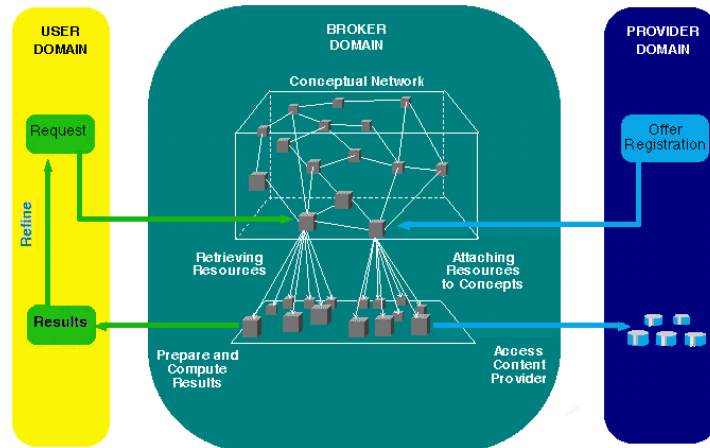


Figura 4-3. Modelo de información de ABS

El modelo de información de ABS que se muestra en la Figura 4-3 se puede descomponer en el dominio del proveedor (llamado modelo Kernel) y el dominio del usuario.

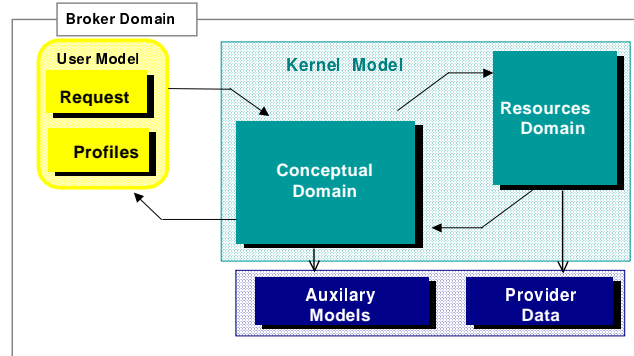


Figura 4-4. Dominio del proveedor (Modelo Kernel)

El dominio del proveedor (Figura 4-4) se descompone en el dominio conceptual y el dominio de recursos:

- Dominio conceptual: Esta basado en el concepto de red conceptual formada por una serie de nodos llamados conceptos y una serie de relaciones entre los conceptos. Enlazados con los conceptos se encuentran los recursos. En la Figura 4-5 se muestra el concepto de red conceptual.
- Dominio de recursos: Contiene todos los proveedores de contenido y sus datos relacionados.

Los principales conceptos relacionados con el modelo de información Kernel de ABS son los siguientes:

- Red conceptual: Estructura jerárquica compuesta por nodos interrelacionados.
- Concepto: Representación de una entidad, información o proceso. Se pueden ver bajo diferentes puntos de vista que representan los diferentes dominios.
- Jerarquía: Para cada dominio los conceptos tienen una semántica especial y están enlazados mediante relaciones formando una jerarquía.
- Relaciones: Los elementos de una jerarquía pueden ser enlazados por tipos de relaciones.

- Objeto sombra: La proyección de un concepto en un plano, asociado al punto de vista de un dominio, se llama objeto sombra.
- Raíz: Un objeto sombra es la raíz de una jerarquía. Un objeto punto de entrada apunta a la raíz.
- Puente: Es un enlace entre dos objetos sombra que representan el mismo objeto.

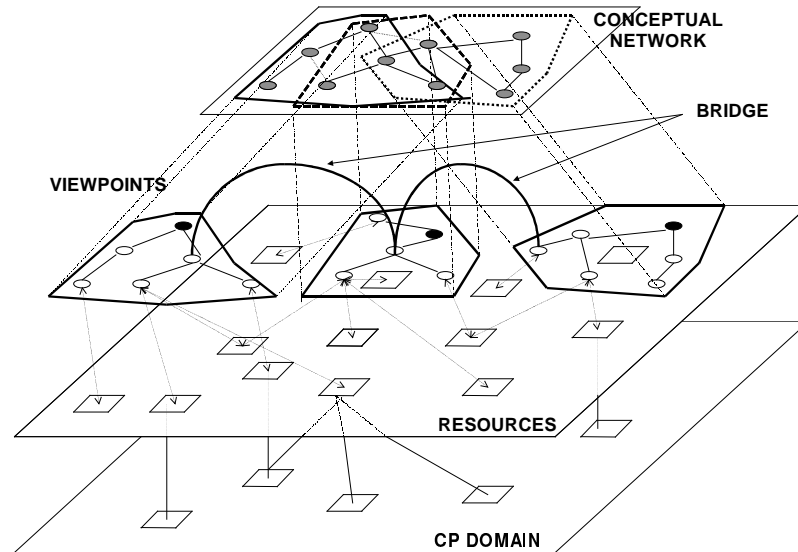


Figura 4-5. Red conceptual

Los principales conceptos relacionados con el dominio de recursos son los siguientes:

- Fuente de información: Un servicio en un proveedor remoto que ofrece información.
- Recurso: Entidad compuesta, mantenida por el intermediario que encapsula información de los proveedores de información.

### 4.1.3 Modelo arquitectónico

Para ABS el servicio de intermediación es un servicio de telecomunicación en el contexto del comercio electrónico que se ofrece encima de un entorno de procesado distribuido. La arquitectura de ABS se basa en la arquitectura TINA-C y el modelo de referencia EC-DTF de OMG.

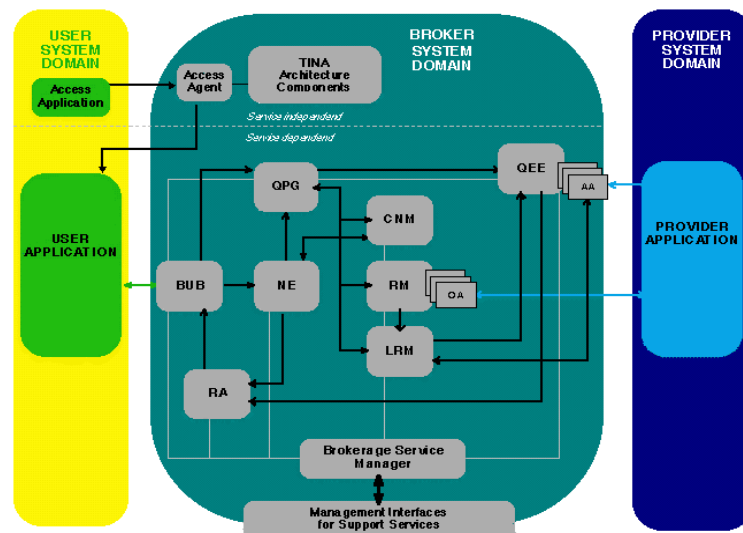


Figura 4-6. Bloques funcionales de la arquitectura de ABS

A continuación en la Tabla 4-1 se describen los bloques funcionales del modelo arquitectónico del proyecto ABS que aparecen en la Figura 4-1.

**Tabla 4-1. Descripción de los bloques funcionales de ABS**

<b>CNM</b>	<b>Conceptual Network Manager</b>	Responsable de la gestión de la red conceptual.
<b>RM</b>	<b>Resource Manager</b>	Bloque que gestiona la descripción de la oferta.
<b>OA</b>	<b>Offer Agents</b>	Ofrece registro de la oferta en RM y opcionalmente en LRM.
<b>LRM</b>	<b>Local Resource Manager</b>	Responsable de la gestión de las bases de datos locales.
<b>BUB</b>	<b>Broker User Block</b>	Representa a los usuarios en el dominio del intermediario. Es el punto final del dominio del intermediario en una sesión de acceso con un usuario. Es accesible desde el dominio del usuario.
<b>QPG</b>	<b>Query Plan Generator</b>	Responsable de la construcción del plan de ejecución correspondiente a una petición del usuario.
<b>NE</b>	<b>Navigation Engine</b>	Para el tratamiento de la navegación.
<b>QEE</b>	<b>Query Execution Engine</b>	Responsable de la ejecución del plan generado por el QPG.
<b>AA</b>	<b>Access Agent</b>	Responsable de la recuperación de la información en el CP y en el dominio local del intermediario.
<b>RA</b>	<b>Result Assistant</b>	Responsable del tratamiento de la presentación de los resultados.
<b>BSM</b>	<b>Broker Service Manager</b>	Controla las interacciones entre todos los bloques funcionales y los componentes relacionados.

## 4.2 Proyecto ABROSE

El proyecto ABROSE (Agent Base Brokerage Services in Electronic Commerce) es un servicio de intermediación para comercio electrónico basado en tecnología de agentes, que recoge los resultados obtenidos en el proyecto ABS (Architecture for Information Brokerage Service).

Los principales objetivos de ABROSE son los siguientes:

- Incorporación de un sistema multiagente para representación de la base de conocimientos.
- Interfaces gráficas para la navegación, petición de resultados, registro y propagación de ofertas.
- Utilización de agentes cooperativos para optimizar la tarea de intermediación.
- Evaluar la incidencia de la tecnología de agentes en el dominio de los intermediarios de información y de las aplicaciones comerciales en general.
- Utilización de Java y CORBA como lenguajes de implementación del sistema.
- Aplicación de Java, CORBA y SNMP para al implementación de la plataforma de gestión del servicio.

Desde el punto de vista funcional el sistema ABROSE, es un servicio de intermediación accesible por Internet mediante el cual el usuario puede realizar peticiones al intermediario o navegar por la base de datos de conocimientos. La tecnología de agentes permite que el intermediario vaya aprendiendo de manera transparente las preferencias del usuario y pueda configurar la lista de proveedores afines de una forma más precisa.

En la Figura 4-7 se muestra la utilización de agentes en el sistema de intermediación de ABROSE. Las interacciones entre los diferentes dominios y el intermediario se basan en la utilización de la tecnología de agentes. Los dominios de usuario y proveedor se comunican con el intermediario mediante un tipo específico de

agentes llamados agentes de comunicación. En el dominio del intermediario los agentes que representan a los usuarios y los proveedores, llamados agentes de transacción, se agrupan para un determinado tipo de especialización bajo el control de un agente de mediación.

El modelo de negocio y el de información de ABROSE están basados en los del proyecto ABS.

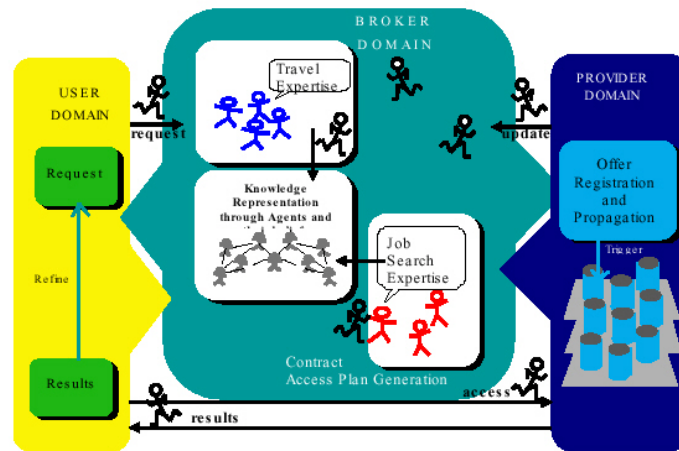


Figura 4-7. Utilización de agentes en ABROSE

Los servicios que ofrece el proyecto ABROSE a todos los usuarios del sistema son los siguientes:

- Aplicaciones: Mercado virtual que ofrece servicios de mediación electrónica con soporte inteligente.
- Elementos de servicio:
  - Compradores: Interacción simplificada, asistencia y notificaciones personalizadas, navegación y peticiones asistidas, visión unificada de ofertas y demandas y propagación de demandas.
  - Proveedores: Propagación de ofertas, adquisición de información de los compradores interesantes para el mercado y adquisición de información de los compradores interesantes para las ofertas de los proveedores.
  - Operación mercado: Aumentar la calidad de la mediación, flexibilidad para adaptarse a los cambios de demandas y ofertas, hacer accesible a los usuarios la experiencia adquirida (memoria colectiva, data mining, etc.).
- Tecnología básica: Tecnología de agentes inteligentes
  - Autonomía: Capturar dinámicamente la evolución del entorno.
  - Cooperación: Red de conocimientos disponibles en el dominio del intermediario.
  - Delegación: Soporte a usuarios para perfiles de peticiones y respuestas.
  - Expertos: Para realizar tareas y subtarear.
  - Razonamiento: Para evaluar sus habilidades propias o externas.
  - Aprendizaje: Evolucionar hacia mejores prestaciones.
  - Autoorganización: Coordinación no centralizada de las tareas a realizar.

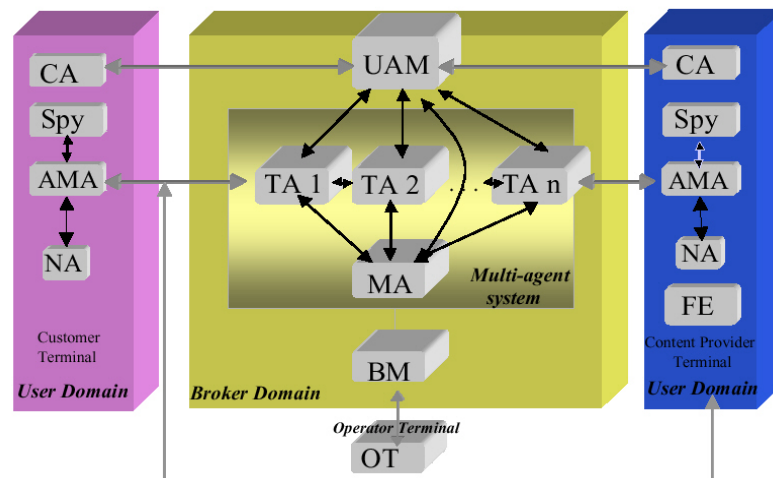
### 4.2.1 Arquitectura

La arquitectura del sistema está basada en dos dominios que son: el dominio del intermediario y el dominio del usuario. El dominio del intermediario se encarga de la función de intermediación y de la gestión del sistema. El dominio del usuario se encarga de la visualización de la información con el usuario (navegación, peticiones, resultados, etc.).

En la Figura 4-8 se muestra la arquitectura de ABROSE donde aparecen los módulos del sistema de los dominios del usuario y del intermediario.

Los módulos que componen el dominio del usuario son los siguientes:

- CA (Asistente de conexión): Es el bloque que ayuda al usuario a registrarse y conectarse al sistema.
- AMA (Asistente de gestión de agentes): Coordina las comunicaciones entre los diferentes módulos del dominio del usuario, así como la comunicación con el dominio del broker.
- NA (Asistente de navegación): Permite que el usuario (proveedor de contenidos o cliente) navegue por el espacio de conocimientos del broker y seleccione los dominios y criterios relevantes para sus peticiones.
- Espía: Se encarga de obtener información de las diferentes peticiones que haga el usuario, con el objetivo de mejorar el conocimiento del usuario que tiene el broker (perfil de usuario), lo cual irá facilitando progresivamente el proceso de adquisición de información más precisa.
- FE (Front End): Es el punto de acceso a la información que posee el proveedor. El usuario obtendrá una referencia para conectarse al FE como respuesta a sus peticiones.



**Figura 4-8. Arquitectura de ABROSE**

Los módulos que componen el dominio del usuario son los siguientes:

- UAM (Gestor de acceso del usuario): Mantiene los perfiles de los usuarios y verifica el acceso a ABROSE. El perfil de usuario tiene como mínimo la información necesaria para permitir el acceso del usuario (identificación y contraseña). Se crea al iniciar el sistema y se mantiene durante todo el servicio.
- BM (Gestor del intermediario): Monitoriza la interacción entre los diferentes módulos del sistema. Se encarga además de la puesta en marcha del sistema.
- OT (Terminal del operador): Ayuda al operador del sistema a realizar la gestión y administración del servicio que provee ABROSE. Muestra el estado de cada bloque facilitando el acceso a los parámetros de gestión.
- MAS (Sistema multiagente): En el dominio del broker, los agentes representan tanto a los clientes como a los proveedores. Cada agente va asociado a un módulo TA (agente de transacción) estando todos los TAs agrupados por conocimientos y controlados por el módulo MA (agente de mediación). El conocimiento del sistema está basado en una red de conocimiento BN formada por el conocimiento de todos estos agentes internos. Cada vez que se hace una petición basada en el conocimiento específico del MA y/o el TA, se localiza a los correspondientes agentes del proveedor. El caso simétrico se produce cuando un proveedor hace una oferta y se localizan los correspondientes agentes de usuario.
  - MA (Agente de mediación): Controlan el ciclo de vida de cada TA y encapsulan todo el conocimiento por ellos adquirido. El MA deberá controlar la creación de TAs asociados a

los nuevos usuarios, así como eliminar los TAs pertenecientes a clientes dados de baja. El MA va a prendiendo progresivamente de las transacciones que se hacen en el sistema.

- TA (Agente de transacción): Representan al usuario en el dominio del broker, almacenando conocimiento sobre él y tratando de conseguir información de otros TAs. Cada TA contiene y mantiene dos redes de conocimiento, una que contiene conocimientos sobre el propio usuario y otra con conocimiento del resto de TAs. El TA es el punto de entrada al dominio del broker, coordinando las comunicaciones entre dicho dominio y el usuario al que están asociados.
- Agentes de conocimiento: Los MAs y los TAs contienen información sobre sí mismos y sobre otros agentes situados en su mismo nivel. Esta información es la que organiza la sociedad de agentes. La base de conocimiento de un MA o un TA es su BN (Belief Network) que se actualiza continuamente para adaptarse a los conocimientos adquiridos durante las diferentes peticiones.

## 4.3 Proyecto COBRA

Los objetivos del proyecto COBRA (Common Brokerage Architecture) son los siguientes:

- Crear una arquitectura abierta para sistemas distribuidos de intermediación on-line.
- Desarrollo y contribución a estándares europeos de arquitecturas de sistemas de intermediación de información.
- Demostración y validación de la arquitectura utilizando cuatro aplicaciones piloto relacionadas con el comercio electrónico.

### 4.3.1 Modelo de empresa

Los principales componentes del modelo de empresa de COBRA (Figura 4-9) son los siguientes:

- El intermediario básico
- Publicidad y relaciones "rendez-vous"
- Relaciones de transacción
- Cadenas de valor y relaciones entre intermediarios
- Servicios de soporte, especialmente terceras partes fiables (TTP)

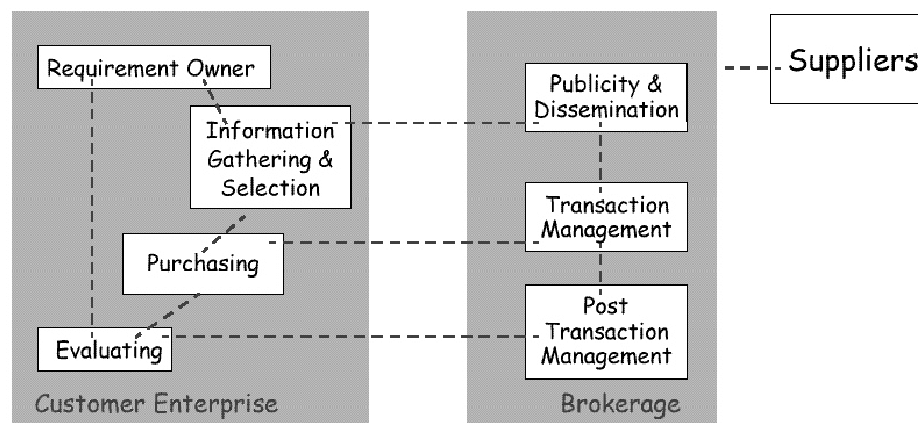


Figura 4-9. Modelo de empresa de COBRA



### 4.3.1.1 El intermediario

En COBRA el intermediario actúa como un creador de mercado. En un contexto de mercado el intermediario tiene las siguientes responsabilidades:

- **Rendez-vous:** Establecimiento de una conexión uno-a-uno entre las muchas posibles entre proveedores y consumidores.
- **Cierre:** Coordinación de las precondiciones y poscondiciones de todas las partes participantes en una transacción y su distribución en el tiempo y el espacio.
- **Recurso:** La responsabilidad de la venta no acaba con la entrega y el pago. Existen responsabilidades asociadas con la descripción o la calidad así como las asociadas con la entrega y el pago.

El cliente tiene las siguientes responsabilidades: localizar, evaluar y seleccionar ofertas, participar en el intercambio y evaluación de los resultados de la entrega en base a los requerimientos y descripción de la oferta original.

El intermediario ofrece las siguientes facilidades: Publicación y mantenimiento del catálogo, gestión de transacciones y control de flujo, registro, gestión de recursos, clasificación de los servicios, provisión de información de mercado y facilitar la entrada al mercado.

Las relaciones entre el intermediario y el resto de entidades puede ser de cuatro tipos dando lugar a diferentes mercados y modelos de negocio :

- **Intermediario neutral:** El intermediario está claramente diferenciado del resto de entidades.
- **Intermediario "push":** Las funcionalidades correspondientes al intermediario y los proveedores de servicio las ofrecen la misma entidad.
- **Intermediario "pull":** Las funcionalidades correspondientes al intermediario y los clientes las ofrecen la misma entidad.
- **Intermediario federado:** Las entidades pueden tener todas las funcionalidades, es decir, de cliente de intermediario o de proveedor.

### 4.3.1.2 Publicidad y relaciones "rendez-vous"

En la componente del modelo de empresa de COBRA Publicidad y relaciones "rendez-vous" (Figura 4-10), podemos identificar los siguientes elementos:

- **Administración:** La publicidad y la provisión de información del mercado están sujetas a la protección del consumidor y a la ordenación del mercado.
- **Fuentes de información:** Las fuentes de información del mercado incluyen los encargados de realizar la publicidad (procurers) sin olvidar el caso más frecuente que sean los propios productores los que se encarguen de hacer la publicidad de sus propias ofertas.
- **Proveedor de información del vendedor:** Proveedor de información que añade valor organizando y diseñando la descripción de la oferta.
- **Proveedor de información del mercado:** Proveedor de información que actúa en nombre del consumidor.
- **Publicidad y difusión:** La entrega de los mensajes son responsabilidad de la empresa de difusión. Los estándares de clasificación de proveedores y servicios ayudan a dar una visión global.

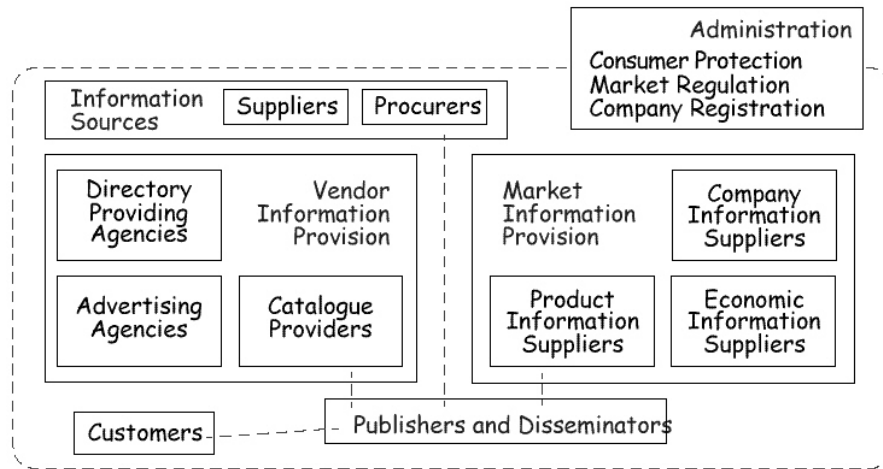


Figura 4-10. Modelo de empresa de COBRA: Publicidad y anuncios

### 4.3.1.3 Relaciones de transacción

La estructura de la transacción COBRA (Figura 4-11) tiene diferentes formas según se comercialicen bienes físicos, contenidos de información o servicios.

La provisión de un servicio en COBRA se ha estructurado en:

- Responsabilidades pre-servicio: pedido, autorización, finalización, recursos y acuerdo.
- Responsabilidades en servicio: gestión, contabilidad y facturación.

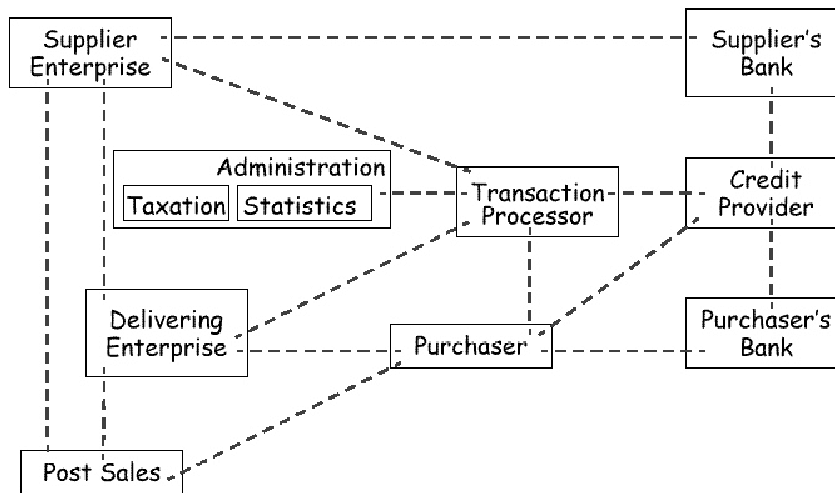


Figura 4-11. Modelo de empresa de COBRA: Transacciones

### 4.3.1.4 Cadenas de valor y relaciones entre intermediarios

Según COBRA un valor añadido específico a una cadena de valor depende de la naturaleza del servicio que entrega, del servicio que consume y de la naturaleza de su inversión (Figura 4-12).

La naturaleza abierta de la operación de mediación depende del enlace entre el proceso de adquisición y las cadenas de valor, de la cooperación y competencia entre intermediarios al mismo nivel de valor, de la coordinación de ofertas entre diferentes niveles de valor y de la provisión de competencia abierta.

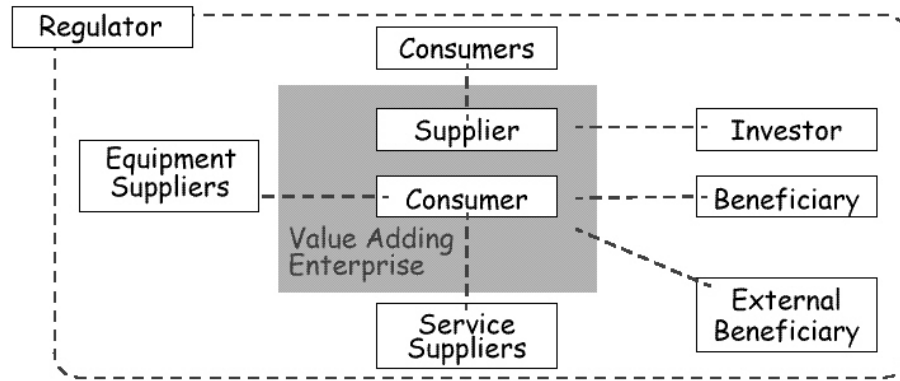


Figura 4-12. Modelo de empresa de COBRA: Cadenas de valor

#### 4.3.1.5 Servicios de soporte como terceras partes fiables (TTP)

Las terceras partes fiables o TTP ofrecen servicios de soporte para realizar actividades comerciales de forma segura:

- Generación y distribución de claves: Ofrece servicios básicos de autenticación, confidencialidad, no rechazo e integridad de las transacciones.
- Servicios de certificación: Ofrece mecanismos para enlazar identidades con entidades legales.
- Servicios de policía y arbitraje: Mecanismos de respuesta en caso de incidencias.

### 4.4 Proyecto GAIA

El objetivo del proyecto GAIA (Generic Architecture for Information Availability) es desarrollar una arquitectura general para facilitar la localización y recuperación de información mediante un intermediario electrónico.

#### 4.4.1 Modelo de referencia

El modelo de referencia de GAIA describe las operaciones y los actores involucrados en la búsqueda, petición y entrega física o electrónica de objetos y servicios en un entorno distribuido de un sistema global de intermediación.

El entorno de GAIA está compuesto por una serie de actores y funciones que se combinan con el objetivo de ofrecer un procedimiento para el acceso y recuperación de información y servicios. Los actores juegan un papel en el proceso que comprende la inicialización y la ejecución de las acciones necesaria para llevar a cabo una transacción.

##### 4.4.1.1 Roles

El modelo GAIA considera que los actores pueden adoptar alguno de los tres primeros roles principales:

- Cliente: El usuario final del sistema GAIA tiene el papel de cliente. Su objetivo es obtener productos o información sobre productos. El cliente es el que inicializa la transacción para obtener una o más acciones GAIA y recibir el resultado de dicha transacción
- Intermediario: Es el encargado de proveer el servicio de mediación a los clientes. Responde a peticiones de los clientes sobre productos o información sobre productos. Los productos que el intermediario ofrece a los clientes pueden proceder de uno o varios proveedores y/o intermediarios.
- Proveedor: Es el propietario del producto solicitado por el cliente. El proveedor genera la información sobre los productos que puede ofrecer y que tiene disponibles el intermediario. El proveedor puede suministrar su producto directamente al cliente o a través del intermediario.

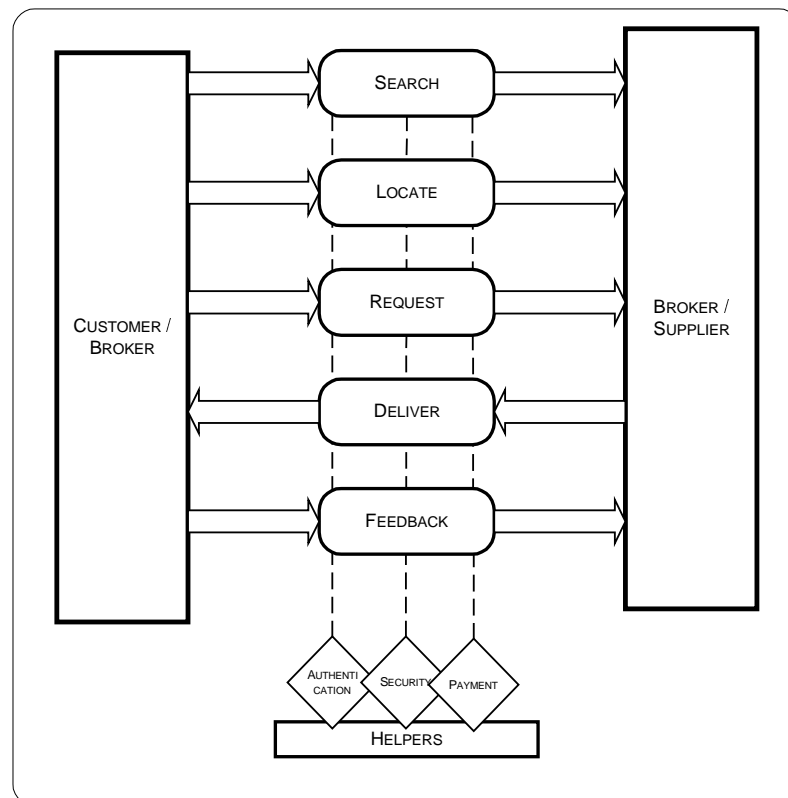
- Ayudantes: Es una aplicación externa al sistema GAIA que ofrece determinados servicios auxiliares como por ejemplo: el servicio de directorio X.500, el servicio de pago electrónico SET o un servicio de autenticación.

#### 4.4.1.2 Acciones

Cada transacción GAIA consta de una o más acciones. Estas acciones son peticiones del cliente al intermediario o al proveedor para realizar cierta operación. Se definen cinco acciones:

- Buscar (Search)
- Localizar (Locate)
- Petición (Order)
- Entrega (Deliver)
- Realimentación (Feedback)

En la Figura 4-13 se muestra el modelo de referencia del proyecto GAIA en el que aparecen las operaciones enumeradas anteriormente.



**Figura 4-13. Modelo de referencia de GAIA**

Los resultados de estas cuatro acciones las devuelve el intermediario al cliente o al proveedor a lo largo de la acción de entrega.

A continuación se describen las entidades de datos que se transfieren en cada acción:

- Buscar: Se utiliza cuando el cliente pregunta al intermediario que busque información en su nombre. Para ello, el cliente da al intermediario una descripción de la información que busca. En función de esa información, llamada metadatos, el intermediario realiza la búsqueda y devuelve el resultado al usuario. El resultado de la búsqueda son un conjunto de identificadores únicos que son referencias a los recursos que satisfacen la descripción dada por el cliente.

- **Localizar:** Cuando el cliente pide al intermediario información sobre productos mediante una referencia que puede ser el resultado de la operación de búsqueda. El intermediario devuelve información sobre el origen de los productos como información de accesibilidad, métodos de entrega disponibles, plazo de entrega, costes, etc. Esta información no se puede considerar final ya que se pueden aplicar descuentos, etc. Los términos finales se establecen durante la fase de negociación de la acción de petición. El intermediario no garantiza la consistencia entre los términos de accesibilidad de la acción de localización y los devueltos directamente por el proveedor en la acción de petición.
- **Petición:** El cliente pide al intermediario o al proveedor que obtenga un determinado producto suministrando información sobre el producto que ha obtenido anteriormente mediante la operación de localización. La acción de petición normalmente tiene una fase de negociación y una de pago. En la fase de negociación el cliente obtiene las condiciones finales de accesibilidad y si las considera satisfactorias procede al pago.
- **Entrega:** Se utiliza cuando el intermediario provee al cliente algún producto que ha solicitado. Este producto puede ser información sobre un objeto físico o metadatos. La acción de entrega puede ser una respuesta a la acción de petición, búsqueda o localización.
- **Realimentación:** Se utiliza cuando el cliente desea revisar la transacción. Puede ser debido a la petición de una nueva entrega cuando ha tenido problemas con la entrega inicial o cuando desea cancelar el pago debido a insatisfacción con el producto o cualquier otra razón.
- **Acciones de soporte:** Es posible que durante la ejecución de las acciones anteriormente descritas sea necesario utilizar alguna actividad de soporte como por ejemplo autenticación, pago y seguridad. La autenticación se utiliza para verificar la identidad de todos actores mediante el intercambio de autenticación. Puede ser necesario realizar un pago durante la ejecución de una transacción GAIA. Las operaciones de seguridad son encriptación, integridad, firma digital, etc.

#### 4.4.2 Modelo funcional

El modelo funcional de GAIA descompone todas las funcionalidades del sistema intermediario en una serie de componentes y describe los roles y las relaciones entre los componentes y la forma como se interrelacionan entre sí. Los elementos claves del modelo funcional de GAIA son:

- **Kernel:** Actúa como intermediario entre las diferentes FUM, como medio de transmisión de primitivas abstractas entre FUM, como almacén local de información, como almacén para datos compartidos para las FUM.
- **Gestor de las unidades funcionales (FUM, Functional Unit Managers):** Se pueden utilizar una serie de diferentes tecnologías para implementar una unidad funcional del sistema intermediario en función del tipo de transacción GAIA. Cada tipo de tecnología tiene su unidad funcional que se utiliza cuando se necesita una tecnología en particular. Para seleccionar la FU (y tecnología) más adecuada, el sistema intermediario necesita conocer cual es la más apropiada a cada caso. Esta función es responsabilidad del gestor de las unidades funcionales. Cada función del sistema intermediario tiene una FUM que se invoca mediante primitivas abstractas por el kernel del intermediario. Esta FUM selecciona la tecnología más adecuada o invoca a la correspondiente FU. La interfaz entre FU y FUM es abierta, independiente de la plataforma y del lenguaje de programación.
- **Unidades funcionales (FU, Functional Units):** El sistema intermediario ofrece una serie de servicios a sus usuarios soportados por sus unidades funcionales como por ejemplo búsqueda, colección de metadatos o conversión de formato. Las operaciones son primitivas abstractas que se pueden mapear en elementos del protocolo seleccionado para soportar la función. Se define una FU para realizar el mapeo entre las primitivas abstractas y las instrucciones del protocolo según el tipo de tecnología escogido. La FU actúa como interfaz entre cada tipo de tecnología y el sistema intermediario. La FU acepta peticiones de primitivas abstractas y las mapea en llamadas a cada tecnología en particular, el resultado de la petición se convierte en las correspondientes primitivas abstractas y es devuelto a la FU.
- **Primitivas abstractas:** La comunicación entre el kernel de GAIA y las FUM y entre las FUM y las FU se realiza mediante primitivas abstractas. Se corresponden con cada operación en particular. Cada FUM importa del kernel un conjunto de primitivas abstractas que representan los servicios que puede recibir de otra parte del sistema o exporta al kernel primitivas abstractas que representan los servicios que puede proveer esta FUM a otros elementos del sistema.

#### 4.4.2.1 Descripción de las FUM

Las funciones más importantes del sistema intermediario son las siguientes:

- FUM de buscar: Acepta peticiones para realizar búsquedas de información de productos que cumplan una determinada descripción del usuario. Devuelve una lista de identificadores de información de productos que cumplen la descripción.
- FUM de localizar: Acepta identificadores de producto y averigua donde los puede obtener. Devuelve una lista de proveedores y ubicaciones del producto.
- FUM de pedir: Gestiona la negociación entre el cliente y el proveedor con el objetivo de alcanzar un acuerdo en los términos de accesibilidad del producto. Después de la negociación acepta la compra del cliente y la reenvía al proveedor. Devuelve una notificación del estado de la petición.
- FUM de entrega simple: gestiona la entrega de ficheros estructurados hacia el cliente.
- FUM de entrega en secuencia: Gestiona la entrega en tiempo real de secuencias de datos multimedia hacia o desde el cliente.
- FUM de pago: Ofrece un mecanismo de pago entre actores.
- FUM de autenticación: Ofrece un mecanismo que permite al usuario probar su identidad frente al sistema intermediario.
- FUM de colección de metadatos: Soporta la colección de información sobre productos y donde son accesibles.
- FUM de cliente: Ofrece una interfaz al usuario que le permite interactuar con el sistema intermediario. También le advierte cuando ocurre un evento relacionado con un determinado cliente.
- FUM de servicio de directorio: Ofrece una interfaz entre el servicio externo de directorio y el sistema intermediario.

En la Figura 4-14 se muestra el modelo funcional de GAIA donde aparecen los gestores de las unidades funcionales (FUM) descritas anteriormente.

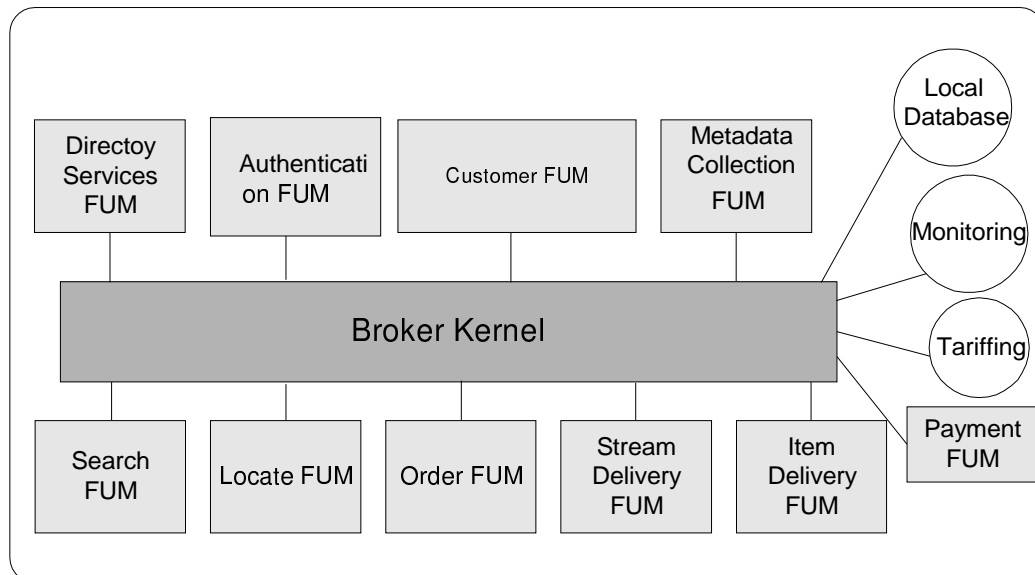


Figura 4-14. Modelo funcional de GAIA: Gestores de unidades funcionales (FUM)

## 4.5 Proyecto OSM

El principal objetivo del proyecto OSM (An Open Service Model for Global Information Brokerage and Distribution) es diseñar un marco global para el comercio electrónico en un mercado virtual. Se centra principalmente en aquellos sistemas con entrega en línea (on-line) de productos y servicios digitales.

Para ello, el proyecto OSM se propone conseguir dicho objetivo en tres etapas :

- Crear un arquitectura abierta para comercio electrónico que soporte catálogo, mediación, negociación, pago, contrato, etc.
- Implementar la arquitectura y el desarrollo de herramientas de soporte a la arquitectura
- Infraestructura pública piloto que permita validar la arquitectura en un escenario real

La arquitectura OSM ofrece una serie de facilidades de comercio como contrato, gestión de servicios comerciales, catálogos, intermediación y agencias que permiten la aparición de mercados electrónicos competitivos, abiertos y globales y ofrece ventajas para:

- Desarrolladores de aplicaciones ya que pueden disponer de un marco para el desarrollo de sus productos. Debe existir un compromiso entre la estandarización y la flexibilidad.
- Consumidores ya que pueden elegir entre un amplio abanico de productos y servicios, a precios competitivos y en un mercado que se adapta rápidamente a sus necesidades.
- Proveedores ya que pueden acceder a un mercado global, a bajo coste, cada día y durante 24 horas. Pueden ofrecer sus productos y servicios de forma más eficiente, acortar su ciclo de vida, publicarlos de forma inmediata, etc.

Los principales resultados del proyecto OSM son los siguientes:

- Arquitectura de comercio electrónico abierta.
- Conjunto de componentes comerciales para soportar comercio electrónico.
- Servicios de gestión de la negociación entre consumidores, proveedores y terceras partes.
- Herramientas de acceso al catálogo de productos y servicios.
- Publicación de la información relacionada con las terceras partes.

### 4.5.1 Arquitectura

La arquitectura desarrollada en el proyecto OSM como marco general para un sistema de comercio electrónico se ha propuesto para su estandarización en el grupo de OMG (Object Management Group) EC-DTF (Electronic Commerce Domain Task Force).

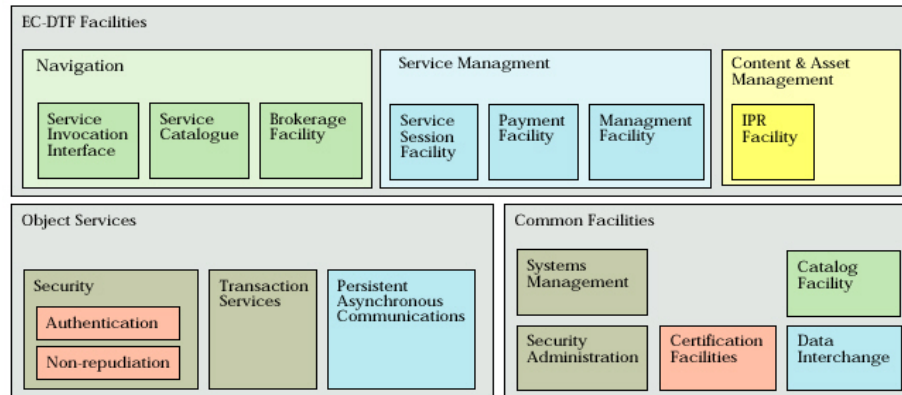


**Figura 4-15. Niveles del modelo OSM**

La arquitectura de OSM (Figura 4-15) para un sistema abierto de comercio electrónico se compone de tres niveles:

- Facilidades orientadas al mercado: Agencia y mediación
- Facilidades de gestión del servicio: Búsqueda, navegación, contrato y servicios de gestión
- Facilidades de bajo nivel: Perfil, selección, certificación y pago

La arquitectura de referencia de OSM pretende desarrollar una interfaz independiente con la intención de convertirse en un estándar internacional. La arquitectura se basa en la plataforma para el diseño de aplicaciones distribuidas CORBA 2.0



**Figura 4-16. Arquitectura abierta para comercio electrónico de OSM**

En la Figura 4-16 se muestra de forma resumida las facilidades de la arquitectura OSM. El modelo de referencia para comercio electrónico EC-DTF, desarrollado en el marco del proyecto OSM, se describe en detalle en el capítulo 3 del estado del arte de la tesis (Ver apartado 3.3).

## 4.6 Proyecto SEMPER

El objetivo del proyecto SEMPER (A Security Framework for the Global Electronic Marketplace) es definir una arquitectura de seguridad general y abierta para un mercado global. Este objetivo general se puede descomponer en una serie de objetivos específicos como son los siguientes:

- Definir un modelo para un mercado global seguro.
- Definir una arquitectura y unos servicios asociados de seguridad.
- Evaluar la arquitectura y los servicios de forma real.
- Difundir los resultados y explotar los resultados del proyecto.

SEMPER es por lo tanto un proyecto especializado en los aspectos de seguridad del comercio electrónico y constituye un referente en el ámbito europeo.



**Figura 4-17. Escenario general de SEMPER**

El sistema SEMPER soporta los siguientes servicios de seguridad:

- Autenticación: Verificación segura de la identidad de todas las entidades.
- Integridad: Garantía de entrega íntegra de los productos y la información.



- **Fiabilidad:** Todos las entidades deben cumplir con sus deberes y obligaciones comerciales.
- **Registro de pruebas:** Pruebas de la recepción y entrega que se pueden utilizar como evidencias en caso de disputa.
- **Pago:** Soportar diferentes métodos de pago (tarjeta, on-line, off-line, etc.).
- **Confidencialidad:** Garantía de confidencialidad en las transacciones.

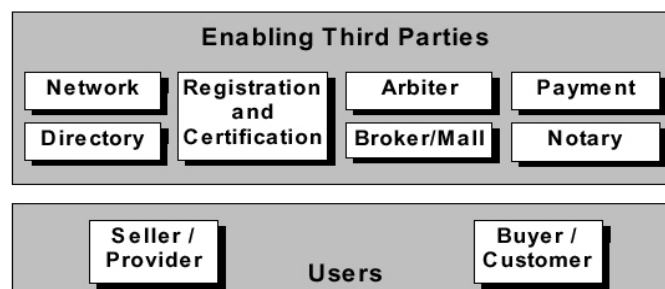
En la Figura 4-17 se muestra el escenario general de SEMPER en el que aparecen los servicios de seguridad, la secuencia de etapas correspondientes a una actividad comercial como una serie de intercambios y transferencias seguras de información entre entidades.

### 4.6.1 Modelo

A pesar de que el marco de SEMPER se diseña para usuarios de comercio electrónico, es decir compradores y vendedores, soporta también otras entidades relacionadas con el proceso de compra. En el marco de SEMPER también aparecen terceras partes fiables (TTP) que tienen funciones de seguridad como notarios o árbitros para evaluar disputas basadas en pruebas digitales.

En el modelo SEMPER (Figura 4-18) aparecen una serie de entidades que juegan unos roles en el desarrollo de la actividad comercial:

- **Usuarios:** Compradores(Clientes) y vendedores (Proveedores)
- **Terceras partes:** Hacen posible la comunicación segura entre los usuarios
  - **Red:** Proveedores de infraestructuras de comunicación utilizadas en el mercado
  - **Directorio:** Una base de datos donde se almacena los datos (atributos) de las entidades como nombre, dirección, clave pública, etc. Es una especie de guía telefónica electrónica.
  - **Registro y certificación:** Las autoridades de registro (RA, Registration Authority) verifican la identidad de los usuarios y las autoridades de certificación (CA, Certification Authority) emiten un certificado digital a las entidades registradas.
  - **Árbitro:** Mediante un protocolo específico de decisiones, el árbitro analiza las evidencias y toma decisiones en caso de disputa.
  - **Intermediario:** Base de datos de entidades presentes en el mercado. Es una especie de páginas amarillas electrónicas.
  - **Mall:** Ofrece una interfaz común a varios proveedores de servicio como servicio de pasarela o servicio de hospedaje de contenidos para proveedores.
  - **Pago:** Proveedores de servicios de pago, instituciones financieras, etc.
  - **Notario:** Soporta sellado de tiempo (time-stamping), firma de contratos, almacenamiento a largo plazo, etc.



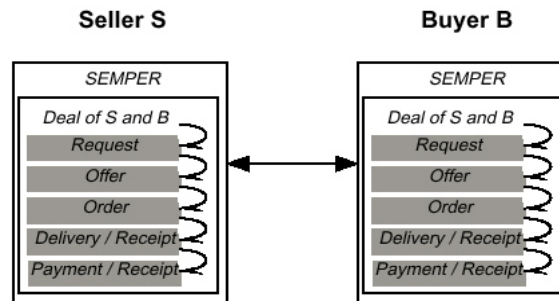
**Figura 4-18. Entidades del modelo SEMPER**

El modelo SEMPER se basa en el hecho de que los aspectos críticos de la seguridad en el comercio electrónico son una secuencia de transferencias o intercambios de información y que los usuarios conocen el estado de sus negocios durante o después de la finalización del proceso comercial.

Una transferencia en SEMPER implica la transmisión de información como un pago o un documento a uno o varios receptores. Una transferencia puede necesitar para su ejecución el intercambio de varios mensajes. En el modelo se distinguen tres tipos de elementos que se pueden transferir: pagos, información firmada como ofertas, pedidos, recibos, contratos, certificados, etc. y entrega de información digital. A cada elemento o a su transferencia se le pueden asociar atributos de seguridad como confidencialidad, no rechazo de origen o destino, etc. Los elementos se pueden agrupar para su transferencia en contenedores. Los atributos de seguridad se pueden asignar a un contenedor. Por ejemplo un pedido y su correspondiente pago se pueden agrupar en un contenedor con un atributo de seguridad de no rechazo de recepción.

Un contenedor es una estructura de datos que puede contener documentos firmados como certificados, recibos, etc., información como bienes o información necesaria para acceder a los bienes o servicios y dinero electrónico.

El concepto de intercambio se utiliza cuando es necesario agrupar varias transferencias para representar una operación indivisible entre una o varias entidades. El pago contra reembolso es un ejemplo de intercambio, el pago se produce solo si se ha producido la recepción del pedido. Los intercambios tienen la garantía para las partes de que la transferencia de un elemento se produce solo si se ha producido la recepción anterior de otro elemento.



**Figura 4-19. Modelo SEMPER**

Comerciar para el modelo SEMPER consiste en realizar una serie de etapas, llamadas transacciones. Un proceso comercial completo debe mantener enlaces entre las diferentes etapas y se debe registrar en todas las entidades que intervienen en el proceso (típicamente en el lado del comprador y del vendedor). En la Figura 4-19 se muestran las etapas de la actividad comercial en el modelo SEMPER que consisten en una serie de intercambios y transferencias seguras. El registro del proceso comercial consiste en guardar la información enviada y recibida durante cada etapa, información completa sobre el proceso de negociación de los atributos de seguridad, la identidad de las partes que intervienen y las relaciones entre las etapas.

La gestión de excepciones entre las entidades y la gestión de las disputas por parte de un árbitro utilizan los registros del proceso comercial en los extremos del comprador y del vendedor. El árbitro puede resolver de forma adecuada las disputas gracias a la inspección de todas las evidencias disponibles.

El modelo descrito anteriormente permite conseguir los siguientes objetivos:

- Múltiples escenarios de negocio.
- Plataforma segura abierta.
- Usuarios pueden gestionar información de forma segura.

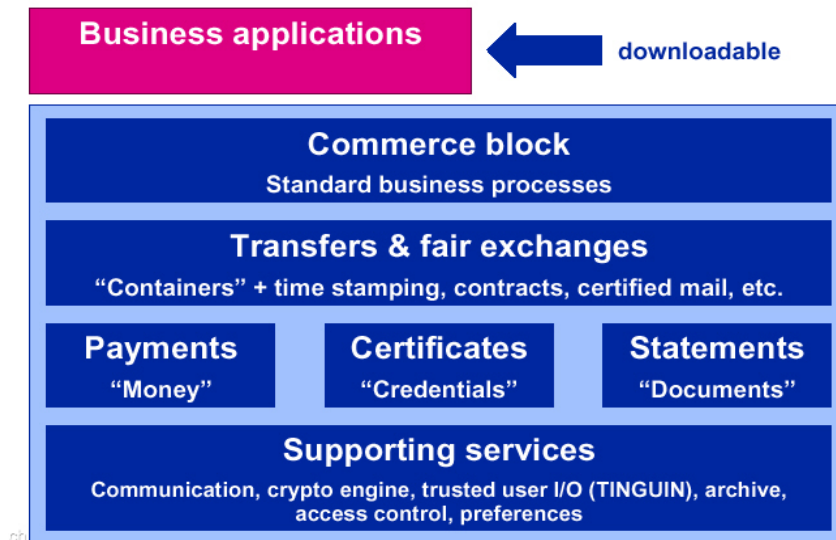
El primer objetivo de permitir múltiples escenarios de negocio se consigue mediante el sistema SEMPER que actúa como una pieza que ofrece servicios de seguridad a las aplicaciones que implementan los procesos comerciales.

El segundo objetivo de ofrecer una plataforma segura para el diseño de aplicaciones de comercio se consigue mediante una serie de interfaces para la integración de implementaciones ya existentes o para el desarrollo de nuevas.

Finalmente el tercer objetivo, de asegurar que los usuarios puedan gestionar información de forma segura, se consigue mediante una interfaz única mediante la cual los usuarios interaccionan con la plataforma segura.

## 4.6.2 Arquitectura

En la Figura 4-20 se muestra el modelo jerárquico de la arquitectura SEMPER, el nivel superior es el modelo de comercio (Commerce Layer), el nivel intermedio es el nivel de transferencia e intercambio (Transfer-and-Exchange Layer), el nivel inferior es el nivel de elementos de negocio (Business-Item Layer) y finalmente los servicios de soporte (Supporting Services) permiten la comunicación segura.



**Figura 4-20. Arquitectura SEMPER**

Las funciones de seguridad ofrecidas por SEMPER están estructuradas en tres niveles y una serie de servicios de soporte que se describen a continuación:

- Nivel de comercio (Commerce Layer): Ofrece servicios de seguridad a las aplicaciones de negocio y finalmente también al usuario para empezar nuevos negocios, navegar dentro o fuera de los negocios en marcha o informar sobre la etapa actual o las anteriores. Mantiene el estado de un negocio y registra su progreso. Los negocios se pueden exportar a un árbitro para la inspección y resolución de conflictos. Abrir un negocio incluye la negociación de la calidad de servicio y en particular de los atributos de seguridad. Además se pueden añadir atributos de seguridad en cada una de las etapas, por ejemplo, si el servicio de confidencialidad no forma parte del conjunto negociado se puede añadir para la entrega de la información. Algunos atributos solo tienen sentido para todo el negocio completo, como por ejemplo el anonimato.
- Nivel de transferencia e intercambio (Transfer-and-Exchange Layer): Gestiona los intercambios y las transferencias. En un intercambio las entidades especifican los elementos de negocio, en forma de descripción, que enviar y que espera recibir. Las entidades también especifican los atributos de seguridad para ese intercambio. Un intercambio únicamente tiene lugar si se cumple que la descripción de los elementos de negocio a transmitir son los adecuados y que los atributos de seguridad necesarios están disponibles. Es posible que para un determinado intercambio sea necesaria la ayuda de un notario, para lo cual SEMPER incluye un protocolo de notario electrónico para la gestión de excepciones. Para las transferencias los elementos de negocio se pueden agrupar en contenedores. Los atributos de seguridad se pueden asociar a los contenedores o a la información almacenada en el contenedor. Por ejemplo se puede enviar un contenedor con el atributo de no rechazo de origen pero internamente se puede enviar información firmada. Contiene los siguientes módulos:
  - Gestor de transferencias: Ensamblado y desensamblado de contenedores.
  - Bloque de servicio de pago: Soporte al pago electrónico.

- Bloque de órdenes: Gestión de la transferencia.
- Bloque del servicio de certificación: Gestión de registro y certificación de usuarios.
- Nivel de elementos de negocio (Business-Item Layer): Gestiona la transferencia de acuerdo con la naturaleza de los datos (pagos, órdenes, información, etc.) enviados y recibidos. La descripción del elemento de negocio se pasa al módulo adecuado para su transmisión y recepción utilizando los protocolos adecuados. Por ejemplo, si el pago se realiza utilizando el protocolo SET, se pasa al módulo SET para que realice la comunicación de la tercera parte con el cliente, el comerciante y la pasarela de pago. Un usuario puede utilizar diferentes métodos de pago, por ejemplo, tarjetas de crédito o pago anónimo que puede gestionar y utilizar en SEMPER. El proyecto SEMPER soporta siete métodos de pago diferentes a través de las interfaces ofrecidas por el nivel de elementos de negocio.
- Servicios de soporte (Supporting Services): Se accede a los servicios de soporte desde los tres niveles mediante una interfaz de usuario fiable. Además de la interfaz fiable se incluyen servicios de criptografía, comunicación segura y contabilidad local. Los servicios de seguridad se utilizan principalmente para la generación de claves, encriptación y firma digital. También se gestionan certificados digitales para utilizar en infraestructuras de clave pública. Los servicios de comunicación ofrecen comunicación de forma unificada y protegen el uso de los servicios de las redes subyacentes. Mediante los parámetros de calidad de servicio es posible seleccionar el canal de comunicación más apropiado. De esta forma la comunicación segura consiste en una extensión con atributos de seguridad como los parámetros de calidad de servicio. Mediante estos servicios se mantiene almacenamiento y recuperación segura de certificados, claves y la información relacionada con la actividad comercial. Mediante el servicio de preferencias el usuario puede establecer sus preferencias de uso del sistema SEMPER. También se dispone de servicios de control de acceso al sistema y de integridad y confidencialidad de los datos mediante los que se verifica los derechos de los componentes de SEMPER y las aplicaciones de negocio antes de permitir el acceso a recursos críticos del sistema. En el proyecto SEMPER se soporta una comunicación anónima que utiliza un esquema de direccionamiento abstracto con direcciones normales y con seudónimo

### 4.6.3 Marco legal

Aunque es imposible prevenir todos los riesgos que comporta el uso de sistemas de comercio electrónico SEMPER propone, para reducir el riesgo, un modelo de acuerdo al que las partes se pueden suscribir, llamado SECA (SEMPER Electronic Commerce Agreement) que permita el desarrollo del comercio electrónico seguro mientras se desarrolla un marco legal apropiado.

El modelo de acuerdo SECA se compone de tres partes:

- Acuerdo: Define el ámbito de acuerdo respecto a áreas de participación y aplicación de transacciones y contiene la obligación de seguir el código de conducta. Regula los contratos suscritos por las partes que comparten un acuerdo SECA. También regula las acciones asociadas en caso de conflicto. El acuerdo debe ser firmado digitalmente por las partes. Se indica como se pueden suscribir nuevas entidades al acuerdo, mecanismos de revocación y listas negras.
- Código de conducta: Asegura la fiabilidad en las transacciones y facilita el comercio electrónico. El código de conducta incluye regulación relacionada con las leyes de competencia, negociación, aceptación de ofertas, protección del consumidor, contenido de los contratos y de las páginas de Internet, privacidad y protección de los datos.
- Guías de uso: Se introduce el concepto de componente que cumple el acuerdo SECA como aplicaciones de comercio electrónico, sistemas operativos o hardware de seguridad, para lo cual se verifica que cumpla los requisitos establecidos en el proyecto SEMPER. Contiene recomendaciones a los usuarios para su autoprotección como utilizar aplicaciones seguras, hardware de seguridad, realizar backups, actualizar las aplicaciones de seguridad, uso de claves, detección de claves comprometidas, etc.