
16

# UFFIZI. SISTEMA DE CONTROL Y GESTIÓN DE IMPRESIÓN EN AULAS INFORMÁTICAS DE LIBRE ACCESO

Tomás Jiménez García
ATICA (Área de Tecnologías de la Información y las Comunicaciones Aplicadas)
**Universidad de Murcia**

Soledad Navarro España
ATICA (Área de Tecnologías de la Información y las Comunicaciones Aplicadas)
**Universidad de Murcia**

Miguel Rodríguez Velázquez
ATICA (Área de Tecnologías de la Información y las Comunicaciones Aplicadas)
**Universidad de Murcia**

## 1. INTRODUCCIÓN

El producto Uffizi es la solución de la Universidad de Murcia, válida y generalizable para cualquier Administración Pública que disponga y gestione Aulas de Libre Acceso con necesidades de cobro de impresión de los usuarios. Es un sistema de control y gestión de impresión basado en el uso de carné inteligente. Soporta distintas plataformas de pago, incluido monedero electrónico.

Uffizi se centra en entornos organizativos con ordenadores en red e impresoras como recurso compartido, donde los usuarios de los ordenadores se identifican ante el sistema con carné inteligente. El sistema permite controlar los trabajos de impresión y todo su ciclo de vida, así como realizar un cobro 'flexible' por el uso de este servicio.

Los clientes de impresión son equipos con arquitectura Win32 donde el acceso está sometido al uso de carnet inteligente y existe un control no sólo de los permisos de acceso sino también el tiempo de sesión.

## 2. CUERPO DE LA PONENCIA

Uffizi es un sistema de uso en entornos con ordenadores en red e impresoras como recurso compartido, donde los usuarios se identifican ante el sistema con carné inteligente. El sistema permite que el usuario imprima desde el pc y hace un seguimiento del trabajo, permitiendo su impresión o no según ciertos parámetros. Cada usuario dispone de una cuota. Esta cuota está formada por un saldo y un crédito.

Antes de realizar la impresión se calcula el coste del trabajo (en base al número de páginas, tipo de impresora, etc.) y se comprueba si el usuario tiene saldo a su favor. En caso de no ser suficiente el usuario puede disponer de crédito de forma que, si el saldo junto con el crédito es superior o igual al coste del documento, éste se imprime. En caso contrario se informa al usuario que su trabajo no puede imprimirse.

El saldo viene dado por dos parámetros: tinteros soft y hard. El saldo puede obtenerse de dos formas:

- **Tinteros hard:** puede adquirirlo desde un Pc con acceso a este servicio o desde cualquiera de las Secretarías Virtuales.
- **Tinteros soft:** este saldo se obtiene gratuitamente en base a distintos criterios definidos en la Universidad.

Uffizi dispone de un sistema de monitorización de estado de impresoras y colas, generando alarmas y enviando información oportuna al personal o responsable que se indique en la aplicación. Soporta envío de alarmas vía sms, correo electrónico, etc.

El control de impresión está situado en el siguiente contexto:

a) Entorno con ordenadores en red e impresoras como recurso compartido
b) Los clientes de impresión son equipos con arquitectura Win32 (NT, 2000 y XP) donde el control de acceso está sometido al uso de carnet inteligente y a las premisas de **SCGina,** que controla no sólo los permisos de acceso sino también el tiempo de sesión.
c) El carnet inteligente utilizado es una tarjeta multiaplicación con monedero WG10 y aplicación universitaria.

d) Soporta plataforma de micropagos con monedero, a través de la red siguiendo las especificaciones del proyecto Sestertium. Es posible configurarlo para otras opciones de pago: cargo desde administrador, pago con banda, etc.
e) Se considerarán impresoras interrogables mediante SNMP.

**Elementos físicos participantes.**

Los elementos físicos participantes en la arquitectura se enumeran a continuación, así como las plataformas existentes o elegidas para cada uno de ellos.

- Cliente de impresión Uffizi con tarjeta.
- Servidor de impresión: plataforma Linux.
- Servidor de pagos: plataforma Win NT Server o 2000 Server.
- Servidores de aplicaciones y de bases de datos: plataformas Oracle 8i, WAS 5.0 y otros.

Pese a especificarse la plataforma, ha sido una premisa de diseño e implementación el desarrollo de software portable, evitando el uso de librerías y estructuras que obliguen la existencia de una plataforma concreta.

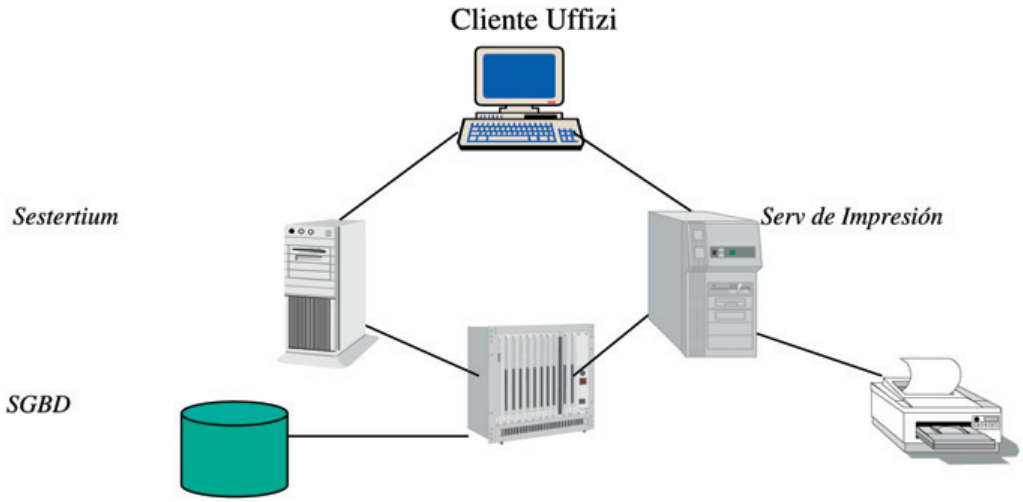


Figura 1. Arquitectura general de Uffizi

**Elementos lógicos**

Los elementos lógicos que intervienen en el sistema son:

a) **Cliente Uffizi** distinguimos:

1. *Módulo SCGina*. Se encarga de gestionar el acceso físico al equipo mediante la tarjeta inteligente y del control de la sesión.
2. *Registro Windows*. El módulo SCGina se encarga de escribir en una zona accesible por otros procesos el DNI del usuario que está actualmente haciendo uso del sistema. Se eligió el registro frente a otras formas de almacenamiento por estar sometido a controles de acceso a nivel de permisos NT.

3. **Comunicación Ufizzi.** Este módulo se encarga de responder a las necesidades de comunicación con el servidor de impresión. En principio, éstas se reducen a la interrogación por parte del servidor sobre el DNI actualmente en el registro.
4. **Servidor ligero HTTP.** La comunicación cliente-servidor de impresión para todos los aspectos relacionados con el control de la impresión se realizará sobre HTTP definiéndose los protocolos de nivel superior oportunos. Se opta por HTTP por la independencia de las máquinas participantes, securización con SSL
5. **Navegador con cliente Sestertium.** En caso de optar por micropagos, el pago para adquirir cuota de impresión se realizará mediante un navegador tradicional, accediendo a una aplicación web de compra y consulta de la cuota de impresión, con protocolos de pago definidos por Sestertium.

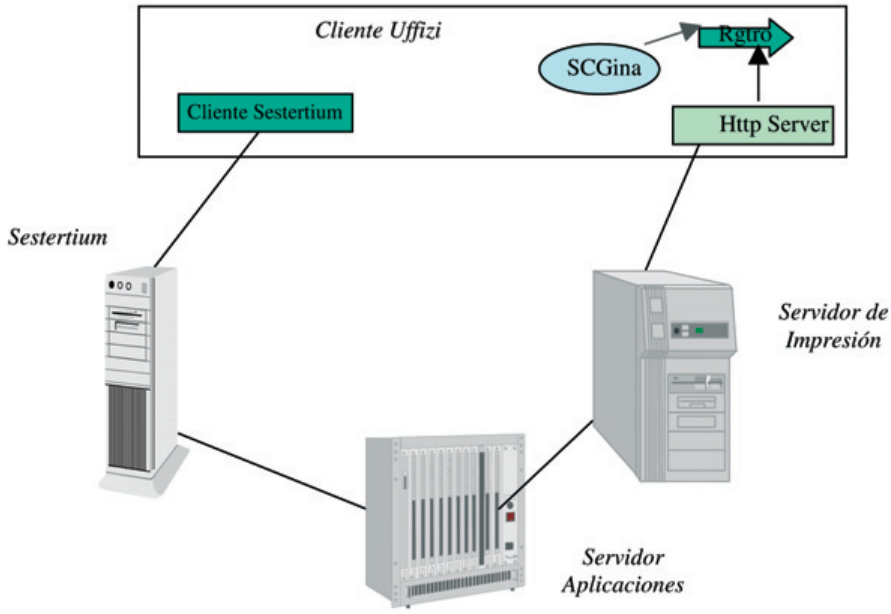


Figura 2. Arquitectura específica de Uffizi

b) Servidor de impresión:
El trabajo enviado a la impresora será recibido en una **cola de dispatching** que se encarga de validar la realización del trabajo, el cliente de impresión nunca tendrá acceso directo a la impresora. Para ello deberá conocer:
- Características del usuario: DNI o identificador
- Características de la impresora obtenidas de la propia impresora y desde base de datos: tipo de papel, IP, puerto, color, tecnología,…
- Características del documento: número de páginas, color deseado, tipo papel deseado
- Seleccionar la impresora final, reenviando a la **cola de impresión** asociada al dispositivo elegido.

- Comprobar las páginas que se han cobrado finalmente y realizar el decremento de la cuota apropiado.

Como servidor de impresión se usa **LPRng** de Linux, modificando los filtros de accounting AS, AF y AE.

La comunicación con la impresora se realizará utilizando **SNMP**.

El documento se envía a la cola de impresión como **PostScript.**

Se ha decidido abstraer el acceso a base de datos llevándolo a otra máquina en la que se desarrolla una aplicación web que responde a las consultas realizadas por el decisor de impresión. Se usan servicios web para interrogar la base de datos.

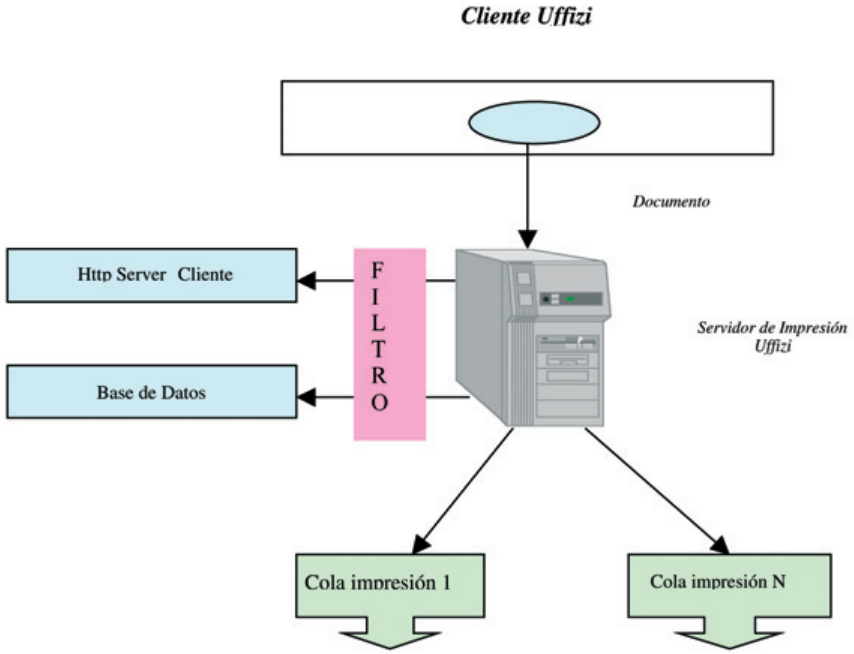


Figura 3. Gestión impresión Uffizi

c) Aplicaciones web y bases de datos

Se requieren varias aplicaciones web para completar el sistema.

- **Aplicación web de compra de cuota (basado en Sestertium)**

El usuario podrá acceder a una aplicación web con SCGina, que permitirá:

- consulta de la cuota disponible.
- consulta del histórico de impresiones realizadas.
- pago de nuevas cuotas: necesita el applet cliente de Sestertium que controlará la interacción con el servidor de pagos.

El acceso a esta aplicación se realizará mediante el interface desarrollado por la Universidad de Murcia para acceso a servicios de Secretaría Virtual desde un PC.

La comunicación subyacente entre servidor de aplicaciones y de pagos está especificada en el proyecto Sestertium.

- **Módulo de acceso a base de datos Ufizzi**

El SGBD se encarga de mantener toda la información y parámetros configurables del sistema, entre la que se encuentra:

- Cuotas de impresión asociadas a usuarios.
- ACLs. Las listas de control de acceso determinan la viabilidad o no de una solicitud de impresión concreta. Para ello, definen la relación entre:
- Características de usuarios (DNI, cuota)
- Características de documento
- Características de impresora
- Franjas horarias y de fecha
- Tabla de impresoras con características

## 3. COMPRA DE CUOTA. SESTERTIUM

Cuando un usuario va a imprimir debe de disponer de cuota para poder realizar esta impresión. Esta cuota está formada por un saldo (tinteros soft y hard) y un crédito. El saldo puede obtenerse de dos formas:

- **Tinteros hard:** puede adquirirlo desde un Pc con acceso a este servicio o desde cualquiera de las Secretarías Virtuales.
- **Tinteros soft:** este saldo se obtiene gratuitamente en base a distintos criterios definidos en la Universidad.

Antes de realizar la impresión se calcula el coste del trabajo (en base al número de páginas, tipo de impresora, etc.) y se comprueba si el usuario tiene saldo a su favor. En caso de no ser suficiente el usuario tiene un crédito de forma que, si el saldo junto con el crédito es superior o igual al coste del documento, éste se imprime. En caso contrario se informa al usuario de que su trabajo no puede imprimirse por falta de saldo.

La compra de cuota realizada en Uffizi son soportados por Sestertium: sistema de micropagos (pagos con monedero electrónico) para tarjeta inteligente integrable con aplicaciones web.

Los sistemas operativos de la tarjeta inteligente necesitan un proceso de autenticación contra un modulo externo –tarjeta inteligente- para completar la transacción. Por motivos de seguridad este módulo almacena unas claves secretas que se usan en la comunicación. La autenticación de la tarjeta consiste en el intercambio de una serie de mensajes entre la tarjeta y el módulo de seguridad en un entorno seguro y local. Sin embargo en las aplicaciones de entornos web esta comunicación debe realizarse en una red, a través de Internet, donde los sistemas son altamente vulnerables.

Sestertium soluciona la limitación de entorno local proporcionando un producto seguro para acceder de forma remota a los módulos de seguridad y un conjunto de protocolos de comunicación para las transacciones implicadas en la operación de micropago. El trabajo analiza los aspectos de seguridad, escalabilidad y flexibilidad relacionados con el programa propuesto y su integración con aplicaciones web de comercio electrónico.

**Protocolo ACCR**

En los micropagos realizados a través de aplicaciones web (Internet/Intranet) es necesario un servidor de pagos, donde entre otras cosas, soporte los módulos Sam. El servidor de pagos controla cada transacción gracias a un protocolo específico diseñado para evitar el fraude.

Sestertium es el servidor de módulos Sam que implementa protocolos de comunicación para transacciones seguras basadas en tarjeta inteligente: micropagos, carga de monedero, actualización de información personal, etc. Para cada transacción se necesitan claves diferentes de forma que el servidor ofrece una matriz de módulos Sam con estas claves secretas.

Cada transacción tiene sus propias requerimientos de securidad de forma que el sistema puede demandar reglas de autorización a un usuario específico. Sestertium proporciona su propio protocolo para este propósito llamado **protocolo ACCR** (Acceso a Claves Criptograficas Remotas).

Este protocolo define 3 fases para una transacción. Ver figura 4:

- La primera fase establece la sesión. El cliente envía un mensaje de petición de conexión que contiene toda la información de la transacción: tipo de tarjeta inteligente, nombre del fichero elemental, nombre del fichero dedicado, tipo de transacción, etc.
- El servidor de pagos consulta la base de datos buscando niveles de seguridad aplicables a la transacción: en las operaciones de micropagos normalmente no se necesita identificación pero las transacciones administrativas implican identificación por parte del usuario y puede ser necesario garantizar de no-repudio.
- Si es necesario la identificación del usuario, el servidor envía una petición de identificación al cliente con un número aleatorio. La clave secreta RSA de la tarjeta se usa para firmar los datos de la operación incluyendo el número aleatorio.
- Cuando los datos firmados llegan al servidor, valida el mensaje recuperando el certificado X509 del servidor LDAP de la Universidad. Si la validación es correcta, el usuario tiene permiso y el servidor dispone de un Sam libre con clave simétrica propia, se reserva éste y comienza la transacción.
- En la segunda fase, dependiendo de las peticiones de conexión se realizan diferentes transacciones.

Finalmente, la última fase se dedica a comunicar los resultados de la transacción.

**Flujo de dinero.**

El monedero de la Universidad de Murcia es un monedero de prepago multi-sector que cumple con las especificaciones del estándar CEN EN 1546. Cuando se realiza un micropago, el e-dinero se descuenta del monedero (débito) y se almacena en el módulo Sam. El estándar CEN EN 1546 define el proceso involucrado de pago y carga en un sistema de micropagos y el flujo de pagos asociados entre participantes. **El proveedor del monedero** es el emisor y tiene toda la responsabilidad en caso de fraude. Este papel le corresponde a Ceca (Confederación Española de Cajas de Ahorros), quien además consolida la transacción individual que llega del servidor de pagos. **El proveedor del servicio** es la Universidad que ofrece servicios al usuario, el cual paga usando su monedero electrónico. El adquirente es el responsable de establecer la comunicación y transferencia de información entre el emisor y proveedor de servicio. Este papel lo ofrece Caja-

Murcia y actúa también de **agente de carga** ya que posee el e-dinero hasta la adquisición de servicio por parte de usuario. Ver figura 5.

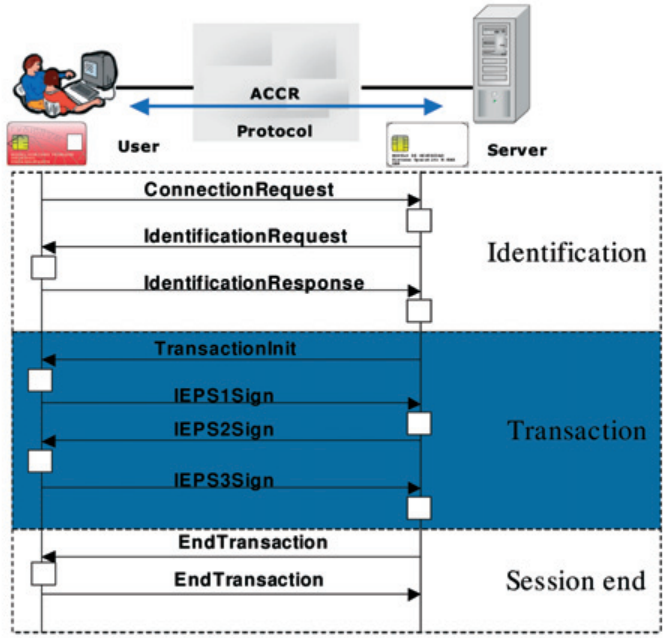


Figura 4: Mensajes de transacciones administrativas y protocolo ACCR

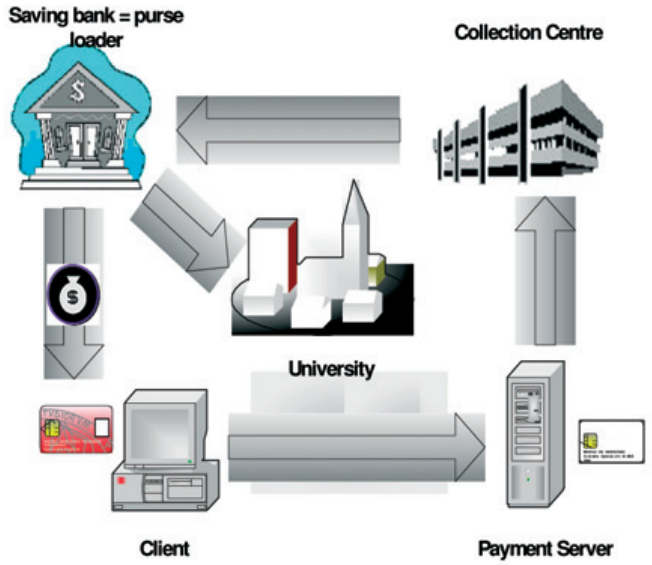


Figura 5: Flujo de e-dinero

Cuando Ceca valida la transacción, envía confirmación a CajaMurcia donde el dinero real se almacenó después de la transacción de carga. Entonces CajaMurcia transfiere la cantidad oportuna de fondos a la cuenta de la Universidad de Murcia.

Sestertium implementa también la comunicación de las transacciones de micropagos mediante el intercambio de fichero vía FTP sobre VPN. El formato del fichero de intercambio es definido por Ceca. Cuando la información está en el host de CajaMurcia, se envían a Ceca usando un método llamado TAF sobre la red propia de los bancos. Ver figura 6.

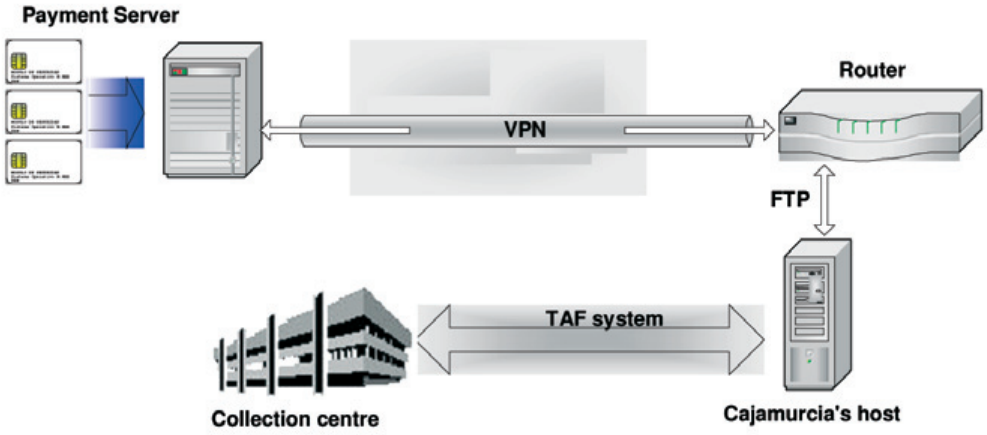


Figura 6. Comunicación segura de datos

**Integración con aplicaciones.**

El servidor de pagos es el programa para micropagos, pero no ofrece en sí ningún servicio. Sestertium se puede integrar con distintas aplicaciones web independientes. El servidor de aplicación ofrece el servicio a través de comercio vía web. Se ha definido un protocolo de comunicación entre el servidor de aplicaciones y el de pago, llamado IAE protocolo (Integración de Aplicaciones Externas), que asegura la validez de los valores y la comunicación de la transacción resultante. IAE trabaja sobre SSL usando certificados X509 proporcionados por una PKI interna.

El propietario de la tarjeta usa un navegador estándar Http para acceder a la aplicación, selecciona el servicio a pagar y finalmente instancia al cliente ACCR (una applet de Java) para realizar el micropago.

La aplicación debió ser registrada en el servidor de pago. Antes de realizar el pago el servidor de pagos envía información al servidor de aplicaciones para validar la transacción. Después de completar la operación el servidor de pagos indica el resultado al servidor de aplicaciones.

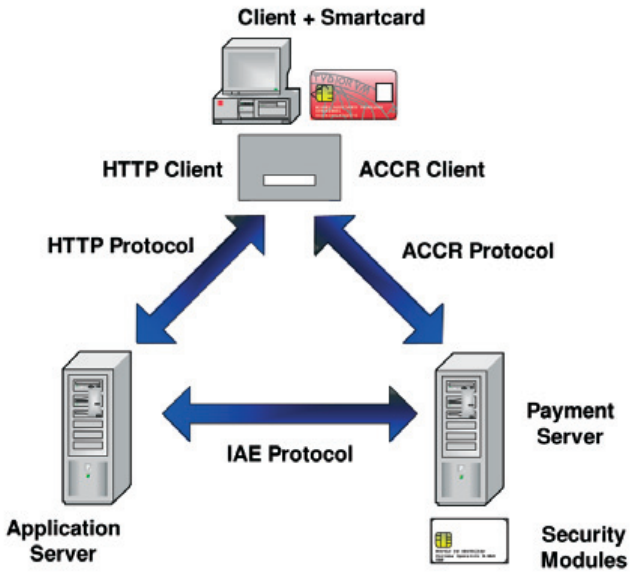


Figura 7. Integración aplicaciones web

## 4. CONCLUSIÓN

Uffizi proporciona un sistema flexible y escalable de control y gestión de la impresión en entornos con acceso libre a los ordenadores. Esta flexibilidad implica desde un control meramente informativo, hasta un pago por parte del usuario por uso del servicio.

Sestertium traslada las ventajas de los micropagos (anónimo, no necesidad de cuenta bancaria y seguridad criptográfica) a aplicaciones web.

Actualmente la Universidad de Murcia ha emitido más de 50.000 tarjetas y anualmente se realizan una media de 800.000 operaciones de pago con monedero electrónico.