Universitat de les Illes Balears

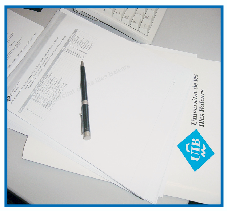
Piloto de Firma Digital de Actas Académicas

B. Serra, J. Ferrer, M. Canals, J. Ferragut

Centre de Tecnologies de la Informació - Universitat de les Illes Balears
Ctra. de Valldemossa, km. 7,5
07071 Palma de Mallorca, Illes Balears, España

www.uib.es/c-calculo

1 Motivación



· El desarrollo de aplicaciones basadas en firma digital permite **consolidar** los **servicios** de una **Infraestructura de Clave Pública.**

· Las **limitaciones** que impone la **presencia física** contribuyen a incrementar la **carga** asociada a los **trámites académicos.**

· La firma tradicional de actas es un proceso **sencillo en el planteamiento** pero **complejo en el desarrollo.**

· Las **nuevas tecnologías** en el ámbito de la **identidad digital** abren vías de desarrollo para una **gestión académica** más **rápida** y **eficiente.**

2 Objetivos

· Estudiar los **requerimientos técnicos** y de **organización** para la puesta en funcionamiento de una **Infraestructura de Clave Pública.**

· **Definir**, **diseñar** e **implementar** un procedimiento de **firma digital de actas académicas** e **integrarlo** en el actual **aplicativo web** de gestión de actas.

· **Generar conocimiento** a través de la experimentación con **sistemas gestores de certificados digitales**, **aplicaciones de firma digital** y **tarjetas inteligentes.**

3 Arquitectura

· La Infraestructura de Clave Pública del piloto está formada por los siguientes elementos:

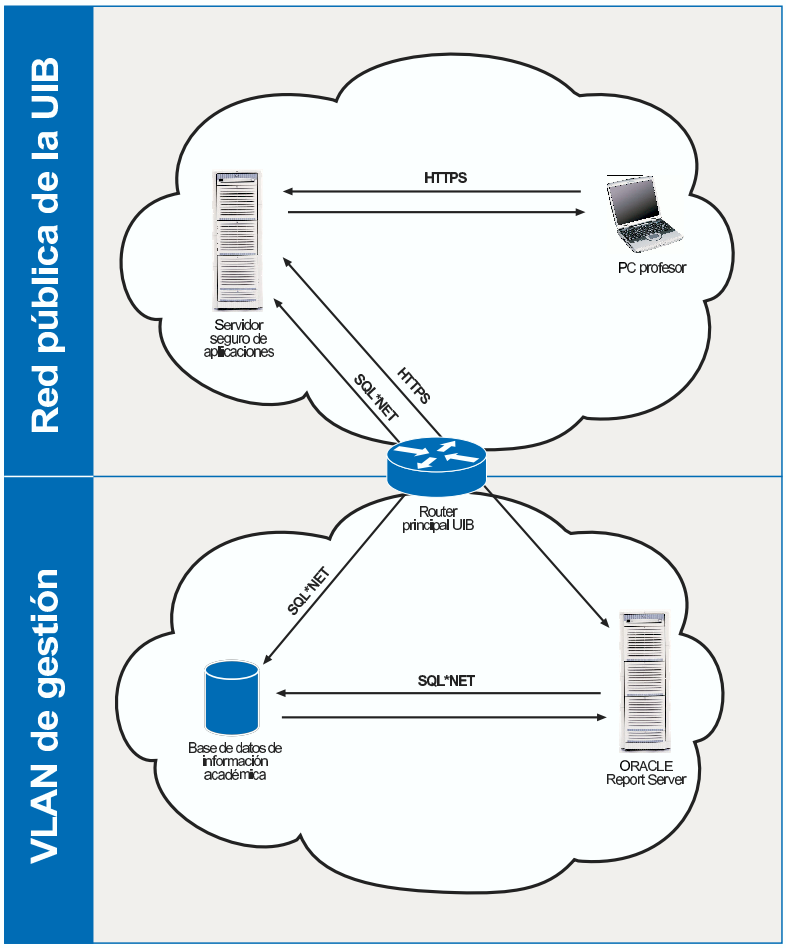
Sistema gestor de certificados:
Procesa las solicitudes de los usuarios autorizados y genera automáticamente los correspondientes certificados digitales. Además, gestiona los procedimientos de revocación y publicación.

Directorio LDAP:
Actúa como repositorio de información personal, certificados digitales y listas de certificados revocados (*CRLs*)

Tarjetas inteligentes:
En una primera fase, su función será la de almacenar de forma segura las claves privadas de los usuarios. En una segunda fase, se experimentará con el uso de criptotarjetas.

· El sistema que permite firmar digitalmente las actas académicas se compone de los siguientes elementos:

Servidor seguro de aplicaciones:
Alberga el aplicativo web de gestión de actas.

Base de datos de información académica:
Almacena la información académica de los alumnos y los procedimientos PL/SQL para realizar búsquedas.

ORACLE Report server:
Esta aplicación es capaz de arrancar procesos *report* de ORACLE y dejarlos a la espera de parámetros para que ataquen a la base de datos. A partir de los registros que ésta devuelve genera informes (en nuestro caso, actas) en formato PDF.