

Integración de aplicaciones/servicios web utilizando firma digital

AC Viviana Fonseca
AC Dalila Romero



Objetivo

Ilustrar cómo es la problemática de incorporar firma digital a un sistema, mostrando qué cambios origina tanto en lo funcional como en la arquitectura del mismo y en la estructura de la base de datos.

Estructura General

- Este trabajo de grado se divide en cuatro módulos
 - Módulo 1: Conceptos Básicos
 - Módulo 2: Montado de la Infraestructura PKI
 - Módulo 3: Implementación
 - Módulo 4: Conclusiones



Introducción

- Surge la necesidad de brindar seguridad en los datos, los servicios, las transacciones realizadas a través de Internet.
- Se investigó la forma de combinar distintas tecnologías para adecuar el módulo de docentes del sistema SIU-Guaraní, y de ese modo brindar en un mismo producto seguridad en la transmisión de datos, autenticidad de cada usuario, y una manera clara y consistente de organizar y manipular información a través de un servicio de directorios.

Introducción

- Incluir firma digital en un circuito administrativo.
- La utilización de Firma digital en una aplicación agrega:
 - Certeza
 - Acciones auditables
 - Consentimiento explícito
 - Manejo de objetos digitales

Módulo 1: Conceptos básicos

- Firma digital
- LDAP



Firma Digital

- Introducción
- Características
- Infraestructura de clave pública
- ¿Por qué usar PKI?



Introducción

- *La firma digital* es un conjunto o bloque de caracteres que viajan junto a un documento, archivo o mensaje, la misma es capaz de acreditar quién es el autor o emisor del mismo (autenticación) y que nadie haya manipulado o modificado el mensaje en el transcurso de la comunicación (integridad).
- La firma digital consiste básicamente en la aplicación de algoritmos de encriptación de datos.

Características

- Autoría electrónica.
- Inimitable.
- Infalsificable.
- Seguridad.
- Indisociable al documento.

Infraestructura de Clave pública

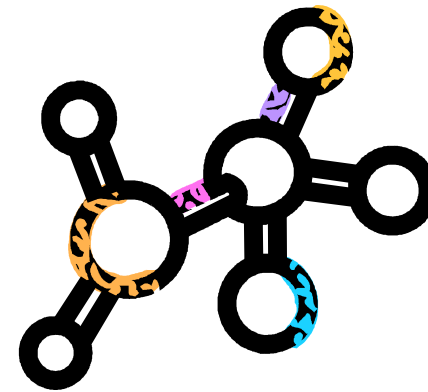
- Infraestructura de clave pública (PKI) es el término utilizado para referirse a la infraestructura de seguridad, basada en criptografía de clave pública, que permite la gestión de **certificados digitales**.
- Un **certificado digital** es un documento digital que identifica a una persona o entidad.
- En una Infraestructura de clave pública, hay que definir y establecer los métodos necesarios para gestionar los certificados digitales.

¿Porqué usar PKI?

- Autentica la identidad, la integridad, la privacidad y el no repudio.
- Autoriza transacciones.
- Disminuye el riesgo de manejo de información.

LDAP

- Introducción
- Características

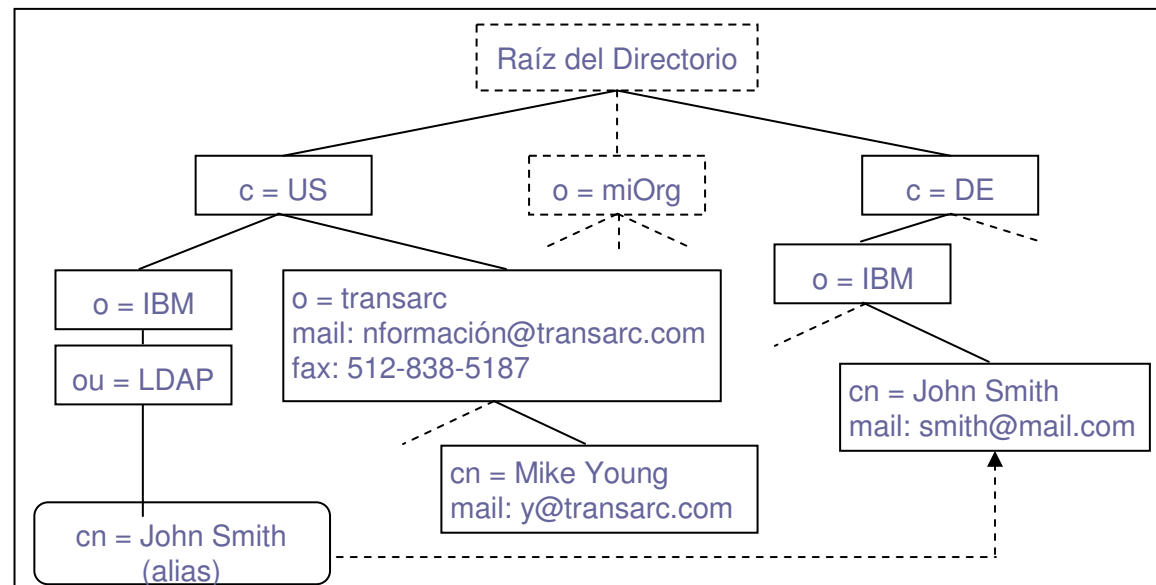


Introducción

- LDAP no define el servicio de directorio en sí mismo, define un protocolo de comunicación.
- Define el transporte y formato de mensajes usados por un cliente para acceder a datos en un directorio X.500-like.
- Es un estándar abierto que ha evolucionado para dar respuesta a estas necesidades.

Características

- Es orientado a objetos
- Originado en el mundo de las bases de datos
- No se limita a una estructura de árbol



Ejemplo de DIT

Características

- Basado en cuatro modelos
 - Información.
 - Nombrado (Naming).
 - Funcional.
 - Seguridad.

Módulo 2: Infraestructura PKI

- OpenCA
- OpenLDAP
- Integración



OpenCA como PKI

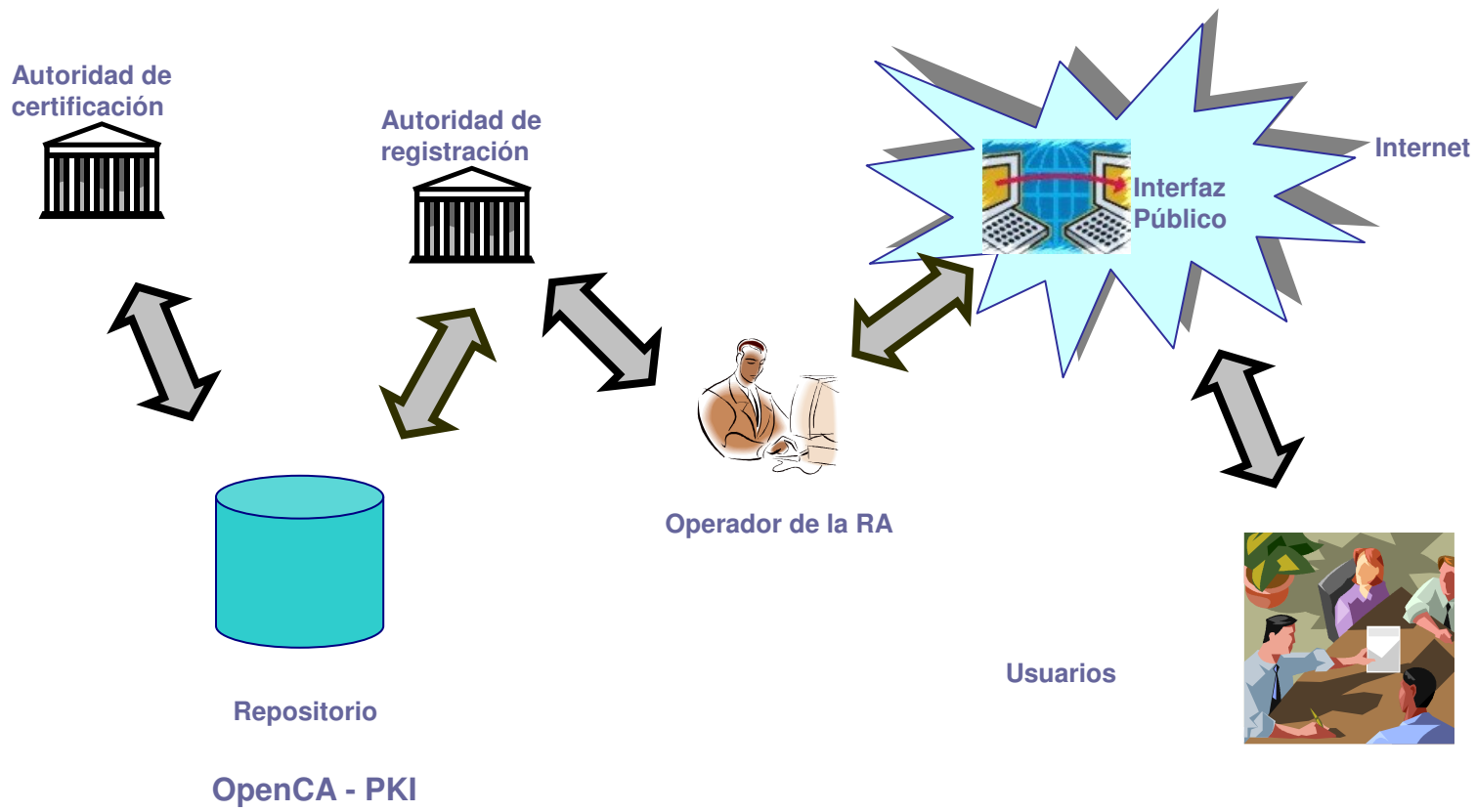
- Introducción
- Funcionalidad
- Consideraciones



Introducción

- OpenCA es un conjunto de programas y scripts que permiten implementar una Infraestructura de Clave Pública.
- Es open source.
- Está compuesta por: la Autoridad de Certificación, la Autoridad de Registración y la Interfaz pública.
- Provee:
 - Verificación de solicitud de Certificados.
 - Procesamiento de solicitud de Certificados.
 - Firma, asignación y manejo de Certificados.

Funcionalidad

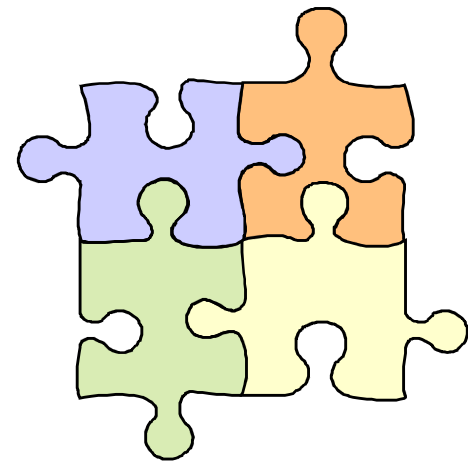


Consideraciones

- Los certificados pueden tener diferentes grados de seguridad.
- Cadenas de CA.

Integración de los componentes

- Introducción
- Cómo obtener un certificado
- Consideraciones

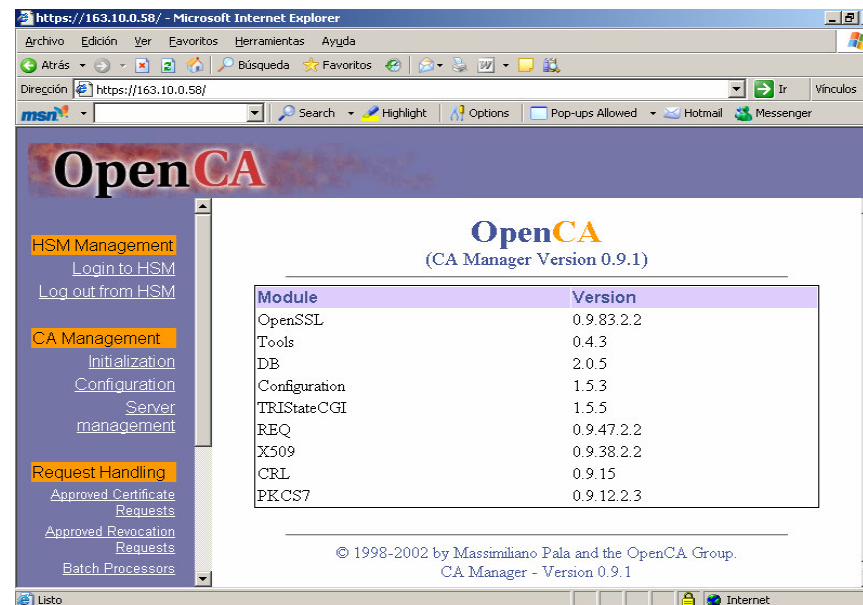


Introducción

- La idea general para el funcionamiento en conjunto de OpenLDAP y OpenCA es la siguiente:
 - el usuario realiza un requerimiento de certificado
 - luego ese requerimiento es tomado desde la RA, para ser aprobado por la misma
 - una vez realizado lo anterior, el requerimiento es tomado por la CA, quien emite el certificado y lo publica en OpenLDAP.

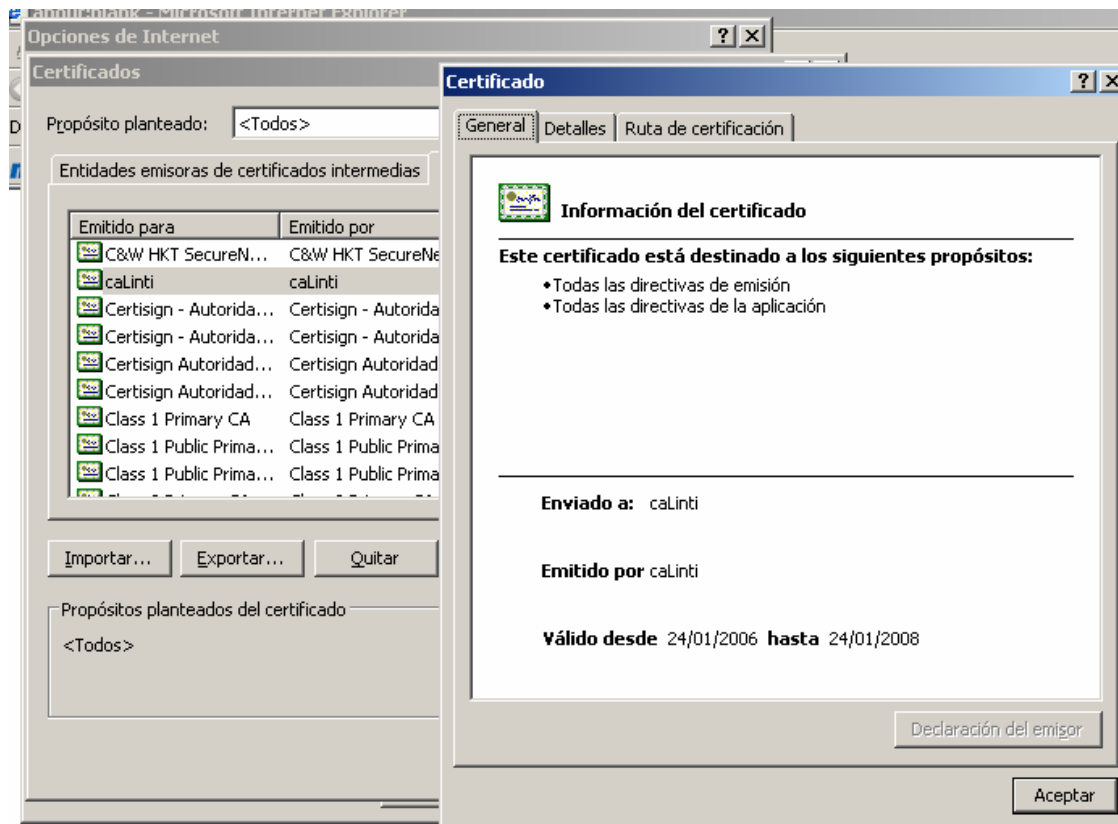
Cómo obtener un certificado

1) Ingresar al sitio de la CA.



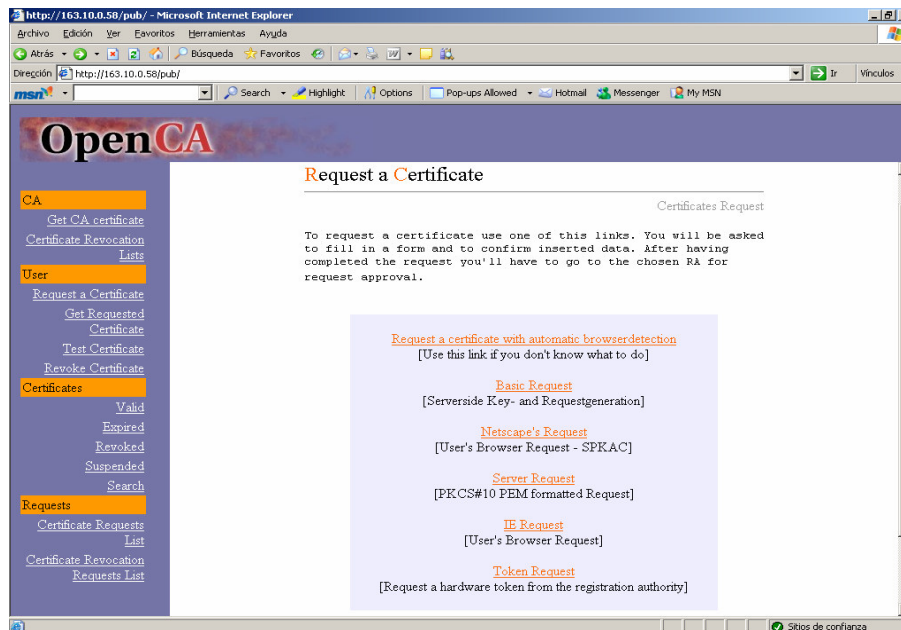
Cómo obtener un certificado

2) Descargar el certificado de la CA.



Cómo obtener un certificado

3) Requerir un certificado.



Integración de los componentes

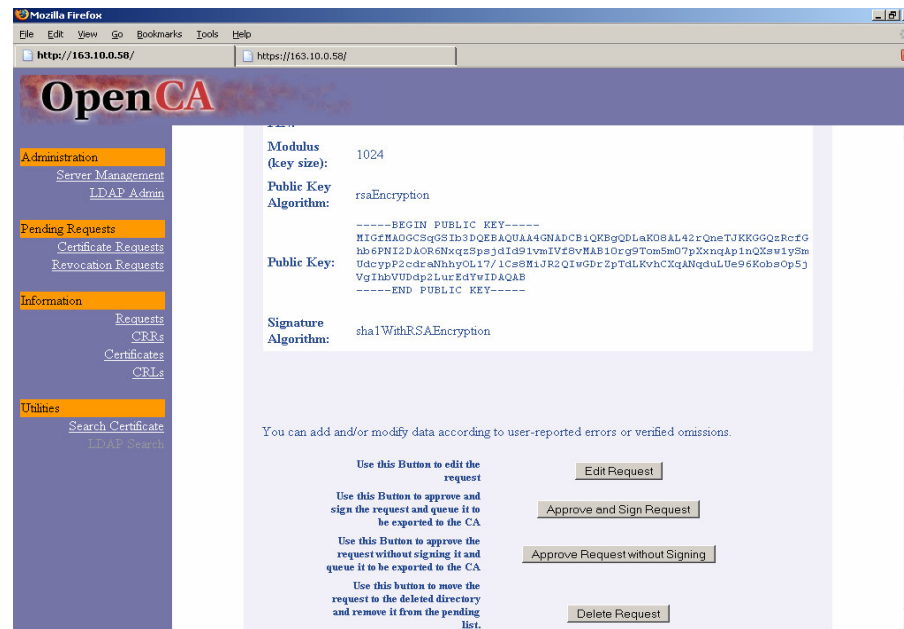
Cómo obtener un certificado

4) Concurrir a la RA.



Cómo obtener un certificado

5) Comprobar la solicitud de certificado.



Cómo obtener un certificado

6) La CA aprueba el certificado.



The screenshot shows the OpenCA web interface in a Mozilla Firefox browser. The browser's address bar displays the URL `https://163.10.0.58/`. The page title is "OpenCA". On the left side, there is a navigation menu with the following sections:

- HSM Management**
 - [Login to HSM](#)
 - [Log out from HSM](#)
- CA Management**
 - [Initialization](#)
 - [Configuration](#)
 - [Server management](#)
- Request Handling**
 - [Approved Certificate Requests](#)
 - [Approved Revocation Requests](#)
 - [Batch Processors](#)
- CRL Handling**
 - [Issue new CRL](#)
- Information**
 - [Certificate Requests](#)
 - [Revocation Requests](#)
 - [Certificates](#)
 - [CRLs](#)

The main content area is titled "Approved Requests" and contains the following text:

Following you can find the request waiting for Certification. This list has been updated on **Tue Jan 24 10:21:53 2006 GMT**.

Below the text is a table with the following data:

No Extra References	
Op. Serial Submit Name	Approved Requested On Role
n/a 1056	emailAddress=jdamiach@yahoo.com.ar, Tue Jan 24 10:07:13 2006 GMT CN=Juan Jose Damianich, OU=Internet, User O=Lenti, C=AR

At the bottom of the page, there is a copyright notice: "© 1998-2002 by Massimiliano Pala and the OpenCA Group. CA Manager - Version 0.9.1".

Cómo obtener un certificado

7) Utilizar el certificado.

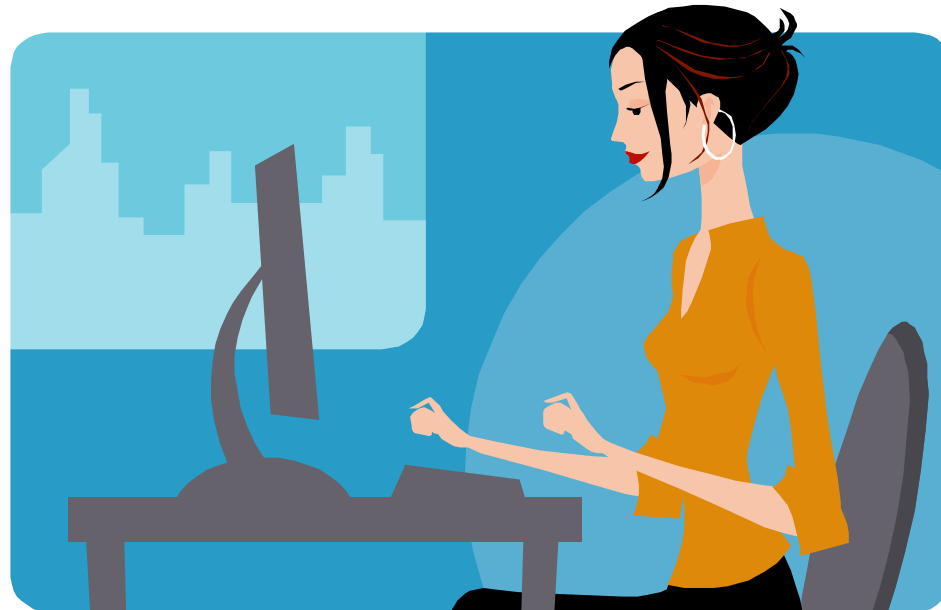


Consideraciones

- **Cómo revocar un certificado**
- **Período de validez de los certificados**

Módulo 3: Implementación

- SIU-Guaraní
- Desarrollo



SIU - Guaraní

Sistema SIU-Guaraní

- Qué es el SIU
- Sistema SIU-Guaraní



¿Qué es el SIU?

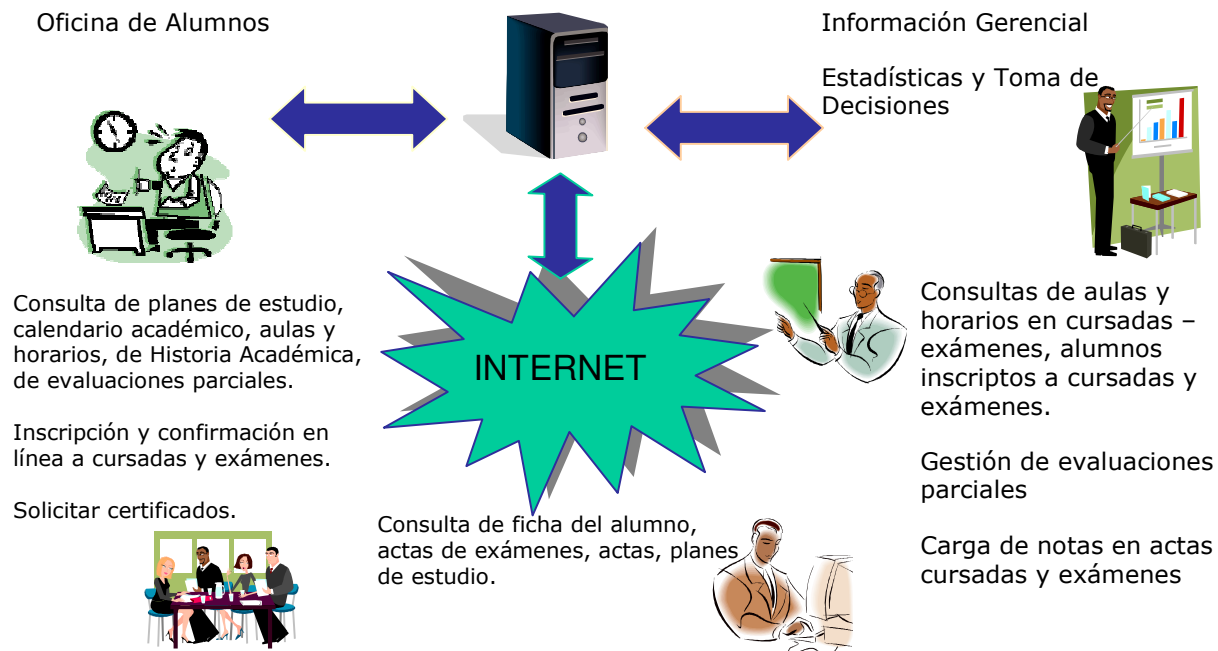
- Sistema de Información Universitario
- Desarrolla e implementa soluciones informáticas y brinda servicios para el Sistema Universitario Nacional.
- Las soluciones y servicios del SIU están en permanente evolución.

SIU-Guaraní

- Es un sistema de gestión de alumnos que registra y administra todas las actividades académicas de la universidad.
- Es un sistema de información que permite mejorar el tratamiento de la información y agilizar los mecanismos de gestión académica.

SIU-Guaraní

- El sistema brinda para su acceso tres módulos diferentes: Gestión, autogestión y Web.



Desarrollo

- Introducción
- Cambios en la estructura y en los procesos de la aplicación
- Especificación
- Funcionalidad obtenida
- Operaciones incorporadas

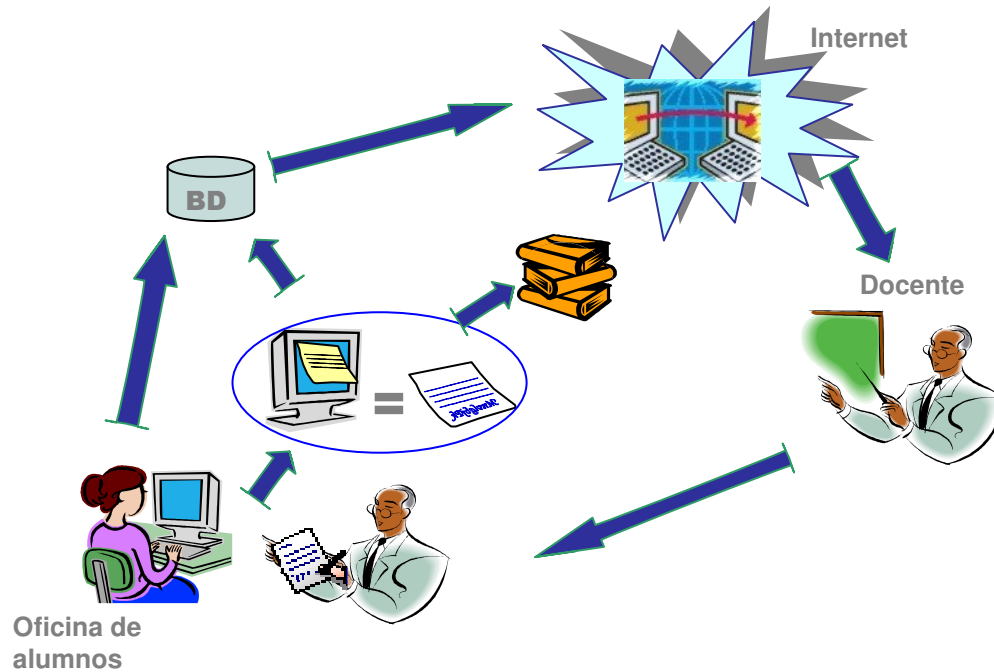


Introducción

- Se adaptó el módulo de docentes del sistema SIU-GUARANI, para facilitar la interacción a través de Internet, entre los docentes de la facultad y la oficina de alumnos en forma segura.

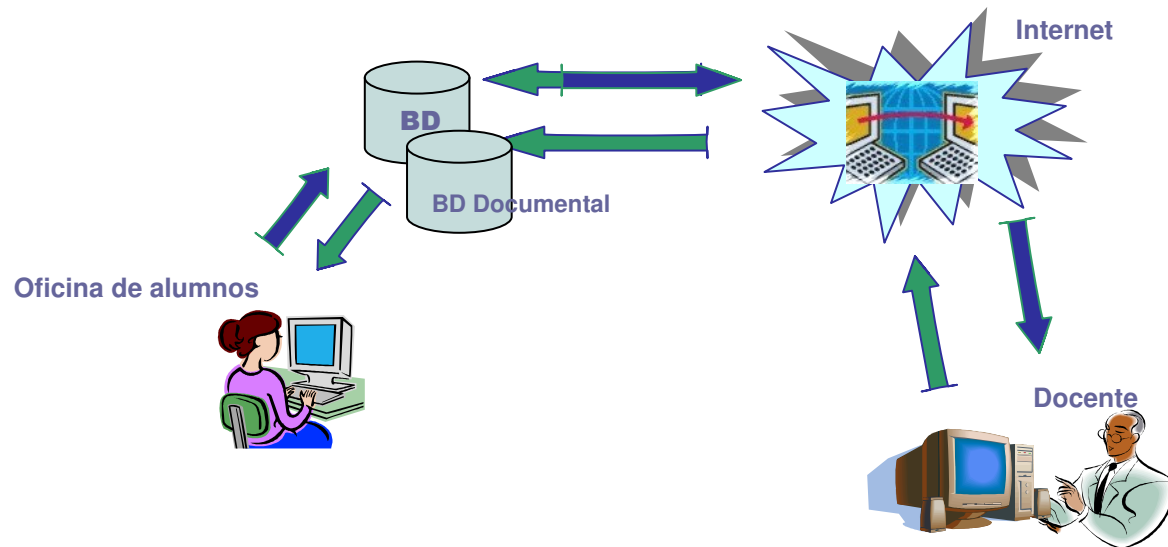
Desarrollo

Cambios en la estructura y en los procesos



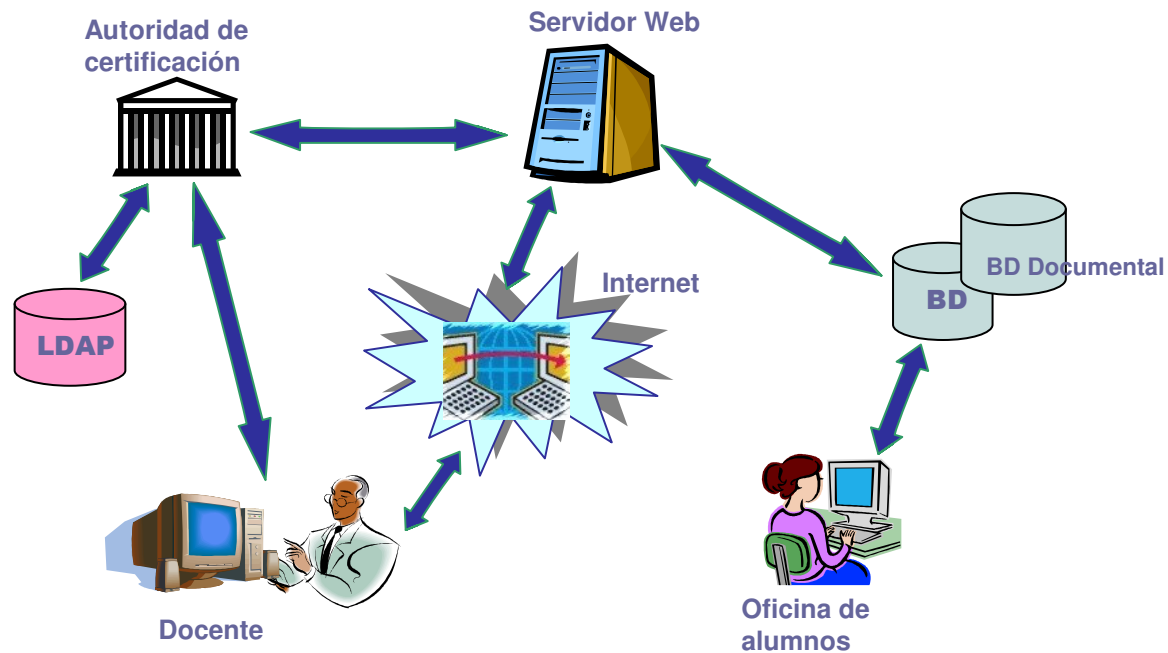
Desarrollo

Cambios en la estructura y en los procesos



Especificación

El docente debe solicitar un certificado



Funcionalidad obtenida

- La incorporación de firma digital a la aplicación modificó y adicionó funcionalidad:
 - El uso de firma digital hace posible que el cierre del acta sea realizado por el mismo docente desde el módulo web a través de las operaciones de firma implementadas.
 - La aplicación administra también documentos firmados.

Desarrollo

Operaciones incorporadas

- Firmar acta de cursada.
- Firmar acta de examen.

Desarrollo

Firmar acta de cursada

- Ingresar al sistema



Desarrollo

Firmar acta de cursada

The screenshot displays the Guarani3W web application interface. At the top, the browser window shows the URL `http://163.10.0.57/guarani3w/`. The main header includes the text "Facultad de Informática" and "Sistema de Gestión de Alumnos - Guarani3W". A navigation menu contains "Iniciar Sesión", "Seguridad", "Finalizar Sesión", "Evaluaciones Parciales", "Consultas", and "Actas". The "Actas" dropdown menu is open, showing options: "Carga de Notas de Cursado", "Carga de Notas de Exámenes", "Firmar Acta de Cursada", and "Firmar Acta de Examen". The "Firmar Acta de Cursada" option is circled in red. Below the menu, a table lists academic records with columns for "Año Acad.", "Per. Lectivo", "Comisión", "Materia", "Acta Reg.", "Acta Prom.", "Folio", and "% cargado". An instruction above the table reads: "Haga click sobre la [icon] que señala el acta de Cursada que desea completar". The user's name "ROMERO, DALILA LUCRECIA" is visible at the bottom of the page. The Windows taskbar at the bottom shows the system tray with the time 18:08.

Año Acad.	Per. Lectivo	Comisión	Materia	Acta Reg.	Acta Prom.	Folio	% cargado
2005	2º cuatrimestre	02	00Q91 - Algebra del Calculo Proposicional	2619	-	1	0%
2005	2º cuatrimestre	01	S0408 - Desarrollo de Software en Sistemas Distribuidos	2528	-	1	65%
2005	2º cuatrimestre	02	S0408 - Desarrollo de Software en Sistemas Distribuidos	2631	-	1	70%
2005	Anual	01	0036L - Conceptos de Lenguajes de Programación	2616	-	1	71%

Desarrollo

Firmar acta de cursada

The screenshot shows a Mozilla Firefox browser window displaying the 'Guarani3W' system. The page title is 'Facultad de Informática' and the main heading is 'Sistema de Gestión de Alumnos - Guarani3W'. The user is logged in as 'ROMERO, DALILA LUCRECIA'. The interface includes a navigation menu with options like 'Iniciar Sesión', 'Seguridad', 'Finalizar Sesión', 'Evaluaciones Parciales', 'Consultas', and 'Actas'. The main content area displays details for an 'Acta de Regularidad' (Act of Regularity) for course 'S0408 - Desarrollo de Softwa' in the year 2005, 2nd semester. It lists 6 students with their respective grades and attendance percentages. At the bottom of the table, there are buttons for 'Firmar' (Sign) and 'Volver' (Return).

Acta de Regularidad Nro.: 2631
Materia: S0408 - Desarrollo de Softwa
Año Académico: 2005
Folio: 1

Comisión: 02
Período Lectivo: 2º cuatrim

Nº	Legajo	Alumno	F. Regular	Asist. (%)	Cond. Regular	Nota	Resultado	P
1	01361/1	DAMIANICH , JUAN JOSE	2006-02-28	100	4		A	N
2	02335/3	ROMERO , DALILA	2006-02-28	0	3		R	N
3	02757/3	COSTA , ALEJANDRO	2006-02-28	100	4		A	N
4	02772/2	FONSECA , MAURO	2006-02-28	0	3		R	N
5	02477/7	POGGI , CARLA	2006-02-28	100	4		A	N
6	03605/1	PEREZ , CAROLINA	2006-02-28	100	4		A	N

[Firmar](#)
[Volver](#)

ROMERO, DALILA LUCRECIA

Done

Desarrollo

Firmar acta de cursada

The screenshot shows a Mozilla Firefox browser window with the address bar containing `http://163.10.0.57/guarani3w/`. The page title is "Guarani3W:index - Mozilla Firefox". The browser's menu bar includes "File", "Edit", "View", "Go", "Bookmarks", "Tools", and "Help". The address bar has navigation buttons for back, forward, refresh, and home, along with a search engine icon and a "Go" button.

The main content area displays the "Facultad de Informática" logo and the text "Sistema de Gestión de Alumnos - Guarani3W". A navigation menu includes "Iniciar Sesión", "Seguridad", "Finalizar Sesión", "Evaluaciones Parciales", "Consultas", and "Actas". The "U.N.L.P." logo is visible in the top right corner.

The central form is a yellow box with the following fields and buttons:

- Certificado:**
- Clave:**
- Aceptar:**

The status bar at the bottom of the browser window shows "Done" on the left and "ROMERO, DALILA LUCRECIA" on the right.

Módulo 4: Conclusiones

- Introducción
- Ventajas y Desventajas
- Líneas futuras de trabajo



Conclusiones y líneas futuras de trabajo

- Introducción
- Ventajas y desventajas de la incorporación de firma digital al sistema SIU-Guaraní
- Líneas futuras de trabajo

Introducción

Utilizar firma digital
no significa solamente
firmar un documento

Ventajas

- Los docentes no necesitan concurrir físicamente hasta la oficina de alumnos para que las actas a su cargo sean cerradas definitivamente.
- Firmar las actas digitalmente facilita futuras funciones de auditoría.
- Ya no es imprescindible mantener un archivo de las actas en papel.

Desventajas

- Los docentes deberán gestionar su certificado digital para poder firmar digitalmente sus actas.
- Se debe permitir que los docentes que no quieran utilizar la firma digital de actas puedan continuar gestionando sus actas como antes.

Líneas futuras de trabajo

- Resolver el problema de que un documento digital sea firmado por más de un profesor.
- Crear los mecanismos necesarios para realizar la auditoría de la base de datos documental.