Single Sign On federado en la UdG e integración con Google Apps

Albert Vergés
Universitat de Girona

Agenda

- Single Sing On web en la UdG
- Federación con Google Apps

Universitat de Girona

Single Sing On **web** en la UdG

- Antecedentes
- Proyectos previstos para 2010/11
- Necesidad del cambio
- SSO analizados
- Por qué escogimos adAS
- Implantación de adAS en la UdG
- Pantallas de login
- Arquitectura para la alta disponibilidad
- Carga del sistema
- Conclusiones

Universitat de Girona

Antecedentes

- Hasta junio de 2011 hemos utilizado SSO propio.
- Desarrollado internamente y hasta la fecha nos ha proporcionado muy buenos resultados.

- **Características**
  - Basado en una **cookie** de sesión y en un conjunto de **webservices** con las operaciones básicas para crear y validar la cookie.
  - **LDAP** cómo única fuente de identidades.
  - Falta de interoperabilidad, **no se ajustaba a ningún estándar conocido**. Gran dificultad para integrar desarrollos de terceros.
  - Seguridad mejorable.
  - Integrada en el portal web corporativo, en Moodle, en Webmail y en la mayoría de desarrollos propios: automatrícula, expediente académico, …

Proyectos previstos para 2010/11

- **Administración electrónica**
  - Gestor documental (Alfresco)
  - Tramitador (OpenSAT / 4tic)
  - Acceso a la Red Sara (federación con SIR)
  - Infraestructura de firma electrónica: Trusted X
- **Tendencia al CLOUD**.
  - Dejar de prestar “servicios commodity” moviéndolos al CLOUD.
  - Intención de mover el correo de los estudiantes a Google
    - **Imprescindible**: Google no debe conocer la contraseña de los estudiantes.
- **Replicar LDAP en Active Directory**

¿ Servirá la cookie UdG ?

NO, sin mucho esfuerzo

Universitat de Girona

Debemos buscar un nuevo SSO

- **Estándar** y fácilmente integrable con desarrollos propios y **externos**
- Que soporte distintas fuentes de usuarios: LDAP, **AD**,…
- Validación de usuarios con contraseña o **DNIe** a través de Trusted X.
- Que permita la **integración** de servicios en la **nube**.
- Y además: Que sea **más fiable y seguro** que la cookie UdG
  - Mejores logs, más trazable.
  - Tokens mejor protegidos.
  - **Más tolerante a caídas**.

CAS - Primera opción

- Preparamos un piloto con CAS
  - Proyecto moviéndose de YALE a JASIG
  - Instalación y configuración asumibles
  - Muchas librerías para “casificar” aplicaciones: Java, PHP, Apache y .NET en beta
- Nos causó muy buena sensación, pero:
  - No existía un cliente oficial para .NET
  - Los compañeros de sistemas nos pedían un solución con soporte para SAML2, preferentemente Shibboleth

Shibboleth. Segunda opción

- Intentamos preparar un piloto de Shibboleth
  - Montamos el servidor.
  - Validábamos contra el SP de demo.
  - No fuimos capaces de configurar un SP local.
  - Documentación en exceso y compleja.
  - Decidimos buscar ayuda externa para evitar dedicar un exceso de horas en sólo investigar.
  - Buscamos ayuda para implantar el piloto de Shibboleth y encontramos a PRISE

Universitat de Girona

adAS - Tercera opción

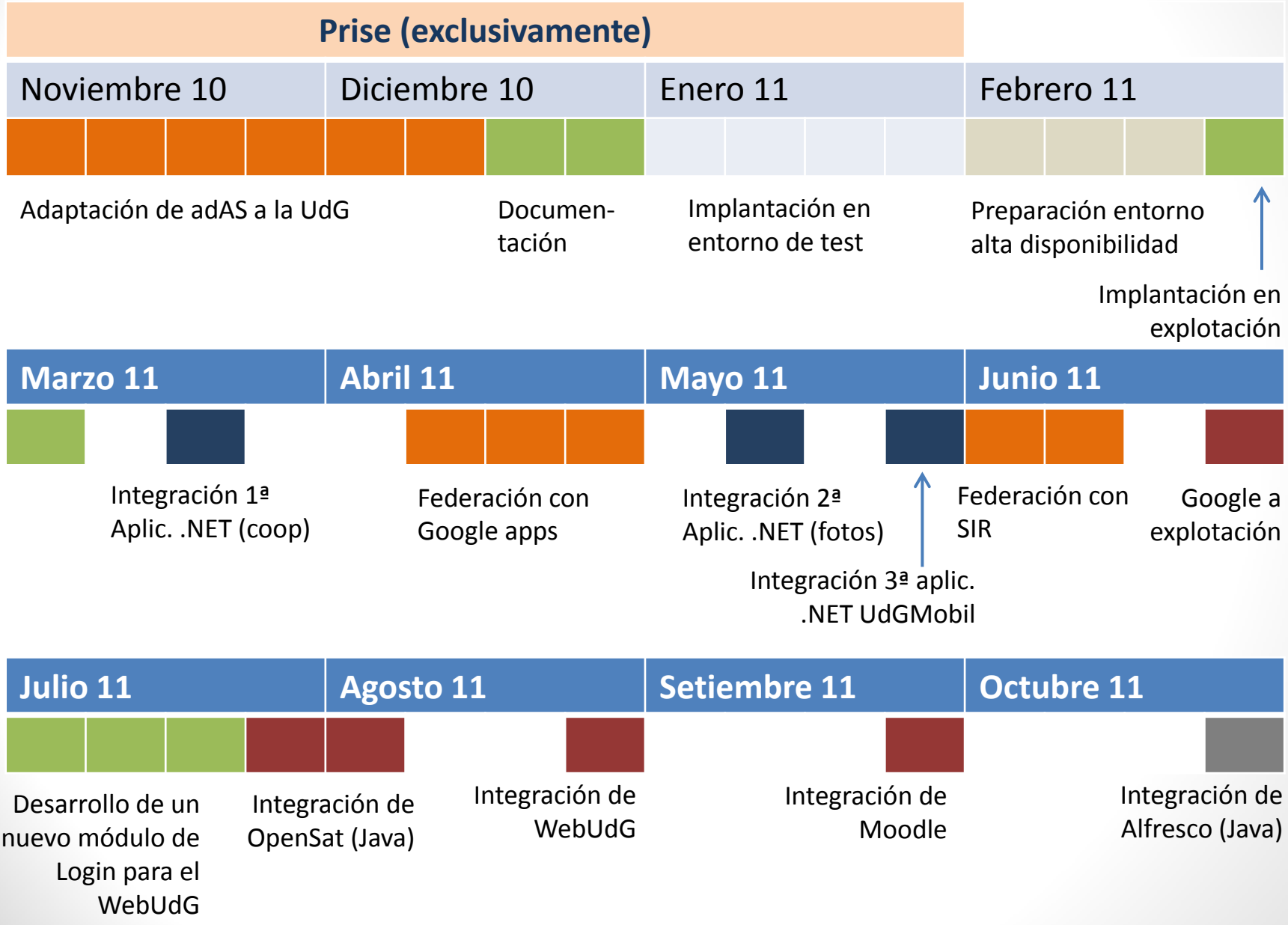
adAS – **ad**vanced **A**uthenticacion **S**erver

- Protocolos: SAML 1.1/Shibboleth 1.3, SAML 2.0, PAPI v1, CAS, OpenSSO.
- Fuentes de datos: LDAP, AD, MySQL, MS SqlServer, …
- Diferentes métodos de autenticación encadenados.
- Librerías para integrar aplicaciones .NET, PHP y Java.
- Atributos definibles para cada SP y usando distintas fuentes.
- Gestión de logs y estadísticas.
- **Interfaz web para la administración**.
- Formularios de login adaptado para dispositivos móviles.

¿Por qué escogimos adAS ?

- Solución casi llaves en mano con un precio razonable.
- Implantación en un plazo corto: **3 meses**.
- Adaptación a los **requisitos** de la UdG.
- Permite la implantación en **alta disponibilidad**.
- Soporta la **federación con Google y SIR**.
- Soporta la validación de DNI a través de **Trusted X.**
- El despliegue de adAS **manteniene la cookie UdG** garantizando la compatibilidad de las aplicaciones no migradas.
- **Documentación personalizada** para la administración y migración de aplicaciones.

Implantación de adAS en la UdG



Universitat de Girona

Login des de aplicaciones web

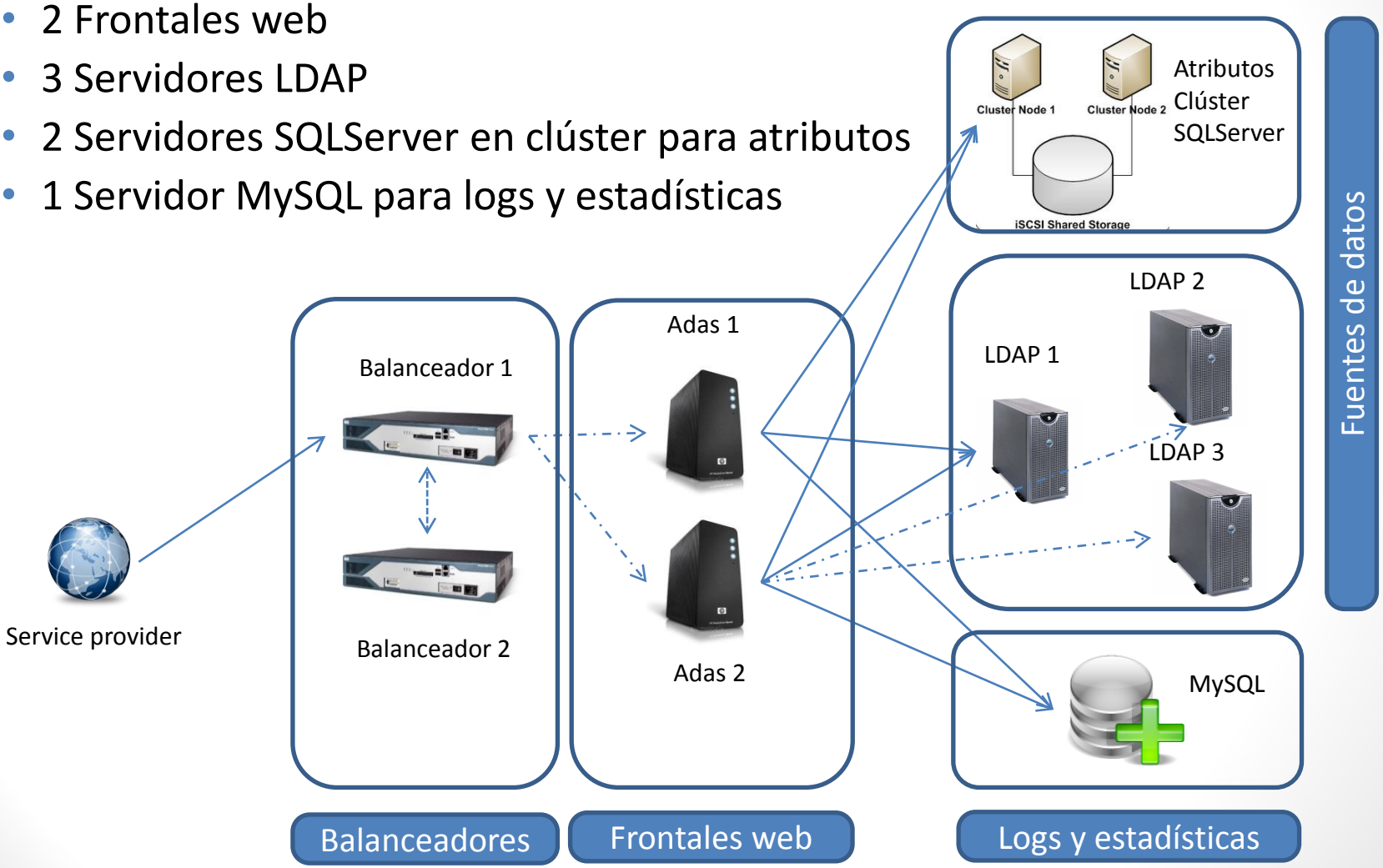
Universitat de Girona

Login desde dispositivos móviles

Universitat de Girona

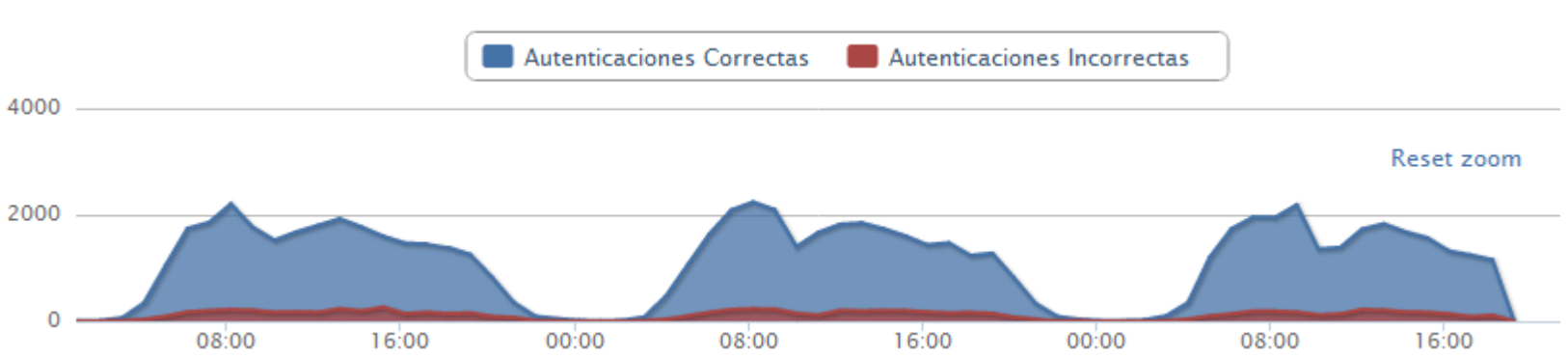
Arquitectura para la alta disponibilidad

- 2 Balanceadores web (activo – pasivo)
- 2 Frontales web
- 3 Servidores LDAP
- 2 Servidores SQLServer en clúster para atributos
- 1 Servidor MySQL para logs y estadísticas

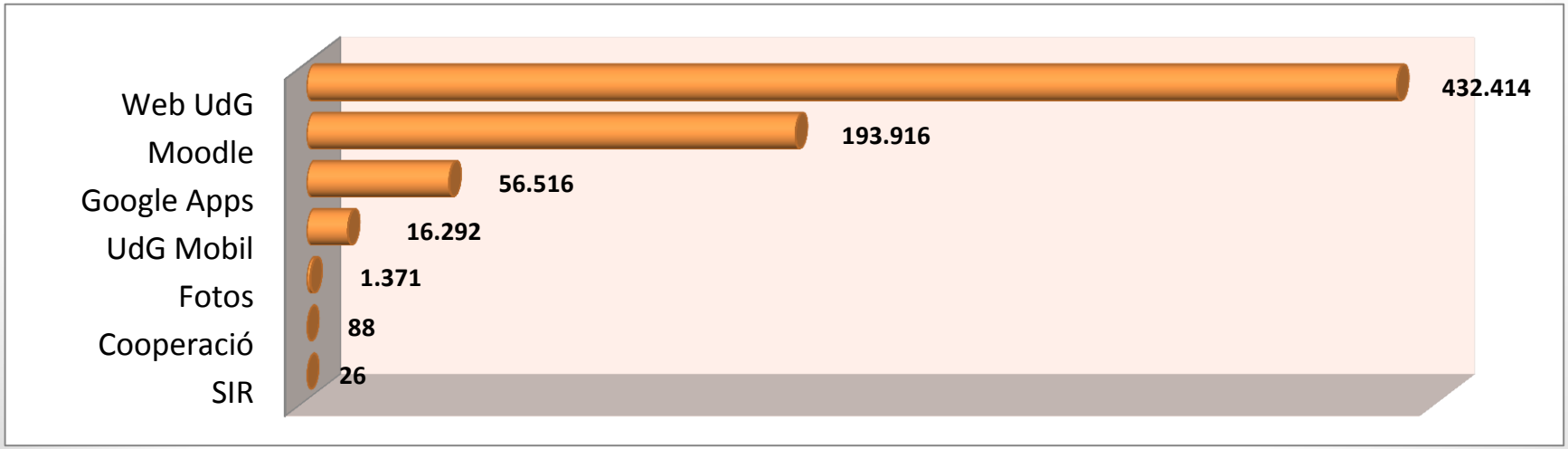


Carga del sistema

- Alrededor de **30.000** autenticaciones **diarias** de lunes a viernes
- 99% de las autenticaciones con protocolo SAML2



- Aplicaciones con más accesos



Universitat de Girona

Conclusiones

- Estamos satisfechos de la elección de adAS.
- Nos ha permitido desplegar el nuevo SSO en un tiempo más que razonable: 1 año.
- El despliegue de adAS ha sido transparente para las aplicaciones no migradas.
- Todos los nuevos desarrollos autentican contra adAS.
- Actualmente adAS ya realiza más del 80% de todas las autenticaciones web en la UdG.
- El próximo año debemos empezar a migrar aplicaciones existentes.
- Hemos tenido pocas incidencias y en todas la respuesta de Prise ha sido muy rápida.

- Mejoras pendientes en adAS
  - Soporte para multiidioma en los formularios de login y los mensajes de error.
  - La instalación de nuevas versiones (nos consta que se está trabajando)

Universitat de Girona

Federación con Google Apps

- Por qué Google Apps
- Correo de los estudiantes 2011
- Proceso de cambio y resultados
- Consecuencias
- Incidencias con el correo @campus
- Implementación técnica
- Federación
- Acceso web
- Acceso móvil
- Conclusiones

Universitat de Girona

¿Por qué Google Apps ?

- El servicio de correo electrónico que puede ofrecer la UdG a los estudiantes no tiene ningún valor añadido respecto a los servicios gratuitos ofrecidos por Google, Hotmail, YahooMail, etc.

- Gestionar el correo de los estudiantes: el spam, los virus,…, manteniendo una calidad de servicio constante supone un coste elevado y casi ningún beneficio.

- Google Apps es más que Gmail; son Docs, Calendar, Chat, Pages,…, y día a día mejora y amplia sus funcionalidades. Además todos sus servicios son usables con la mayoría de dispositivos móviles.

- Evaluamos Windows Live y, aunque como servicio informático tenemos mucha infraestructura Microsoft, creímos que sería más atractivo para los estudiantes la opción de Google.

Correo de los estudiantes / 2011

- **Dejamos de proveer correo electrónico con infraestructura UdG a los nuevos estudiantes**.
- Les ofrecemos la posibilidad de darse de alta como usuarios del Google Apps for Education de la UdG: campus.udg.edu
- **@Notificación**: Les preguntamos en qué dirección de correo electrónico quieren recibir las notificaciones de la UdG.
- A partir de enero, comunicaremos a los antiguos estudiantes que deben abandonar el correo UdG y les animaremos a darse de alta en Google apps.

Universitat de Girona

Proceso de cambio y resultados

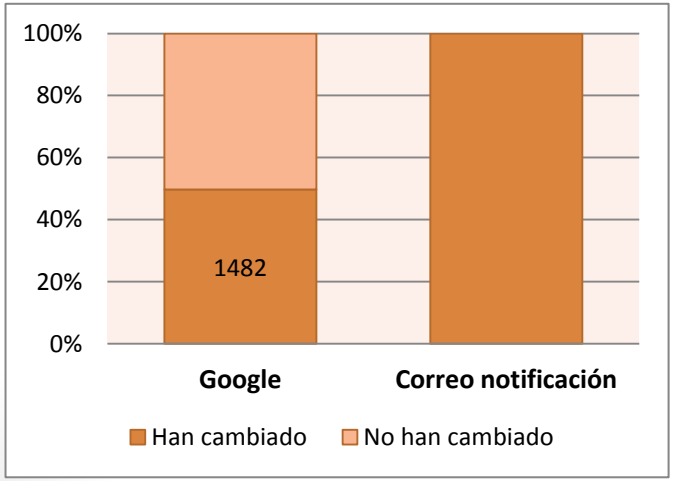
Alta en Google Apps UdG: campus.udg.edu (3.187 estudiantes)

- Durante la matrícula.
- En cualquier momento pueden solicitar el alta desde “identidad digital” en la intranet.

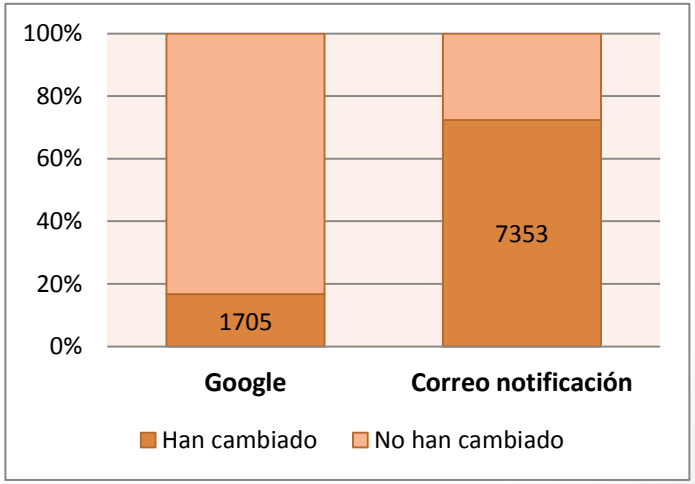
Correo de notificación:

- Durante la matrícula.
- En cualquier momento pueden actualizar la dirección donde desean recibir las notificaciones desde “identidad digital” en la intranet.

Estudiantes de primer curso



Resto de estudiantes



Universitat de Girona

Incidencias correo en google

CERO

Confusiones, consultas

Alguna

Estudiantes que se dan de alta en @campus y definen @notificación distinto esperan recibir las notificaciones en @campus.

Dudas de cómo sincronizar el correo desde dispositivos móviles

Implementación técnica

15 minutos aprox.

Altas

Matrícula

Identidad digital

Base de datos de peticiones

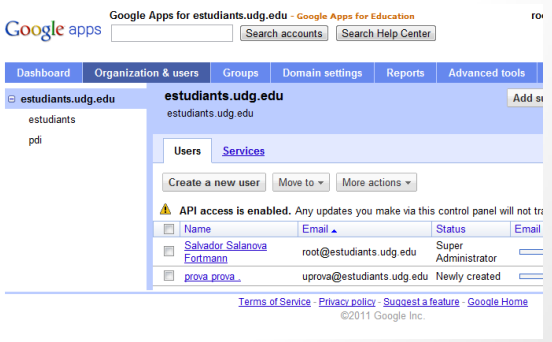
Batch altas **cada 5 minutos**

Username
Nombre
Random pwd.

Llamamos a las **APIS** de Google en **PHP**

Marcamos en LDAP que el estudiante tiene correo @campus

Bajas y modificaciones



Sincronizador LDAP de Google
(de momento) **se lanza manualmente**

Universitat de Girona

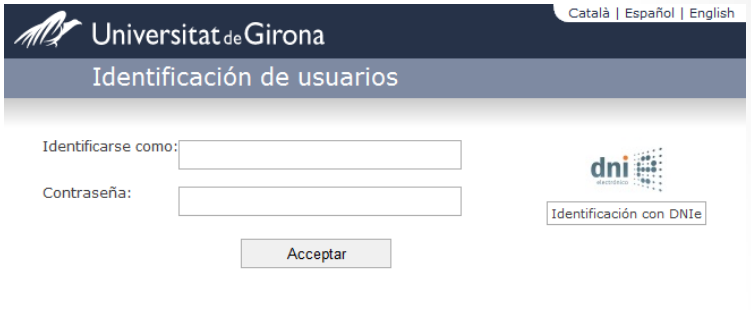
Federación con Google Apps

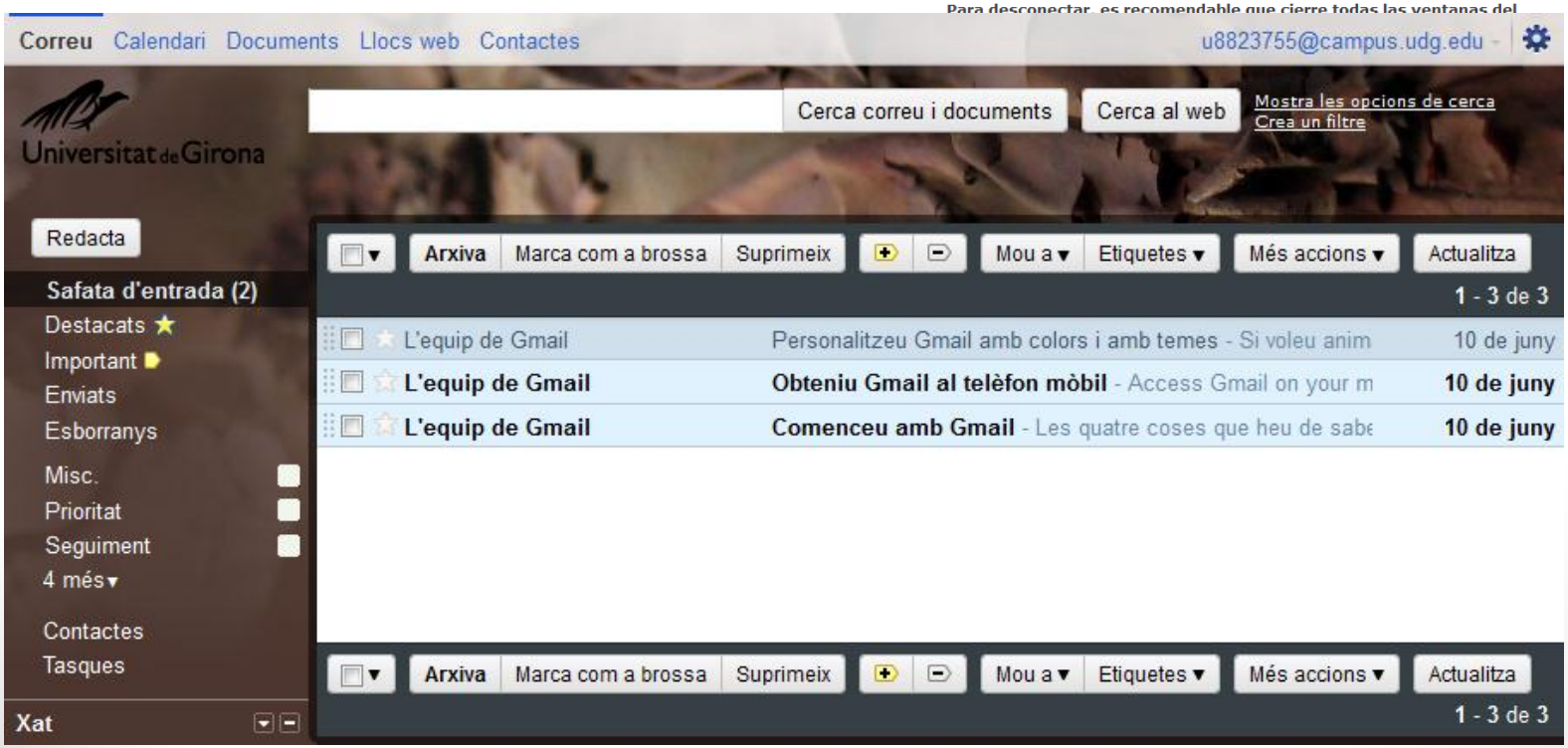
- Federación a través de **adAS**
- Protocolo para la federación **SAML 2.0**
- Google es el Service Provider
- Complejidad de la federación: **NINGUNA**
  - Sólo hay que seguir el manual de adAS

Acceso web

URL de entrada:

http://correu.campus.udg.edu
http://calendari.campus.udg.edu
http://docs.campus.udg.edu





Universitat de Girona

Acceso desde dispositivos móviles

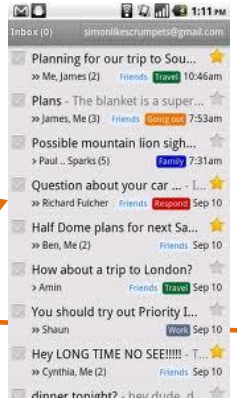
Primero
El estudiante debe definir una nueva contraseña para su cuenta en Google

Llamamos a las APIS de Google en **.NET**

Nueva contraseña “interna”

Identidad digital
En la intranet

Segundo
El estudiante debe configurar la cuenta en su dispositivo



Universitat de Girona

Conclusiones

- Los estudiantes prefieren usar su correo personal antes que añadir una nueva dirección a su “lista de cuentas”.
- El cambio del correo de notificación tiene un impacto importante y nos obligará a no retrasar el proyecto de eNotificador para garantizar la entrega de las notificaciones importantes.
- Es difícil conocer el estado de las altas y bajas en Google debido a que estas se replican entre servidores y se debe esperar cierto tiempo a que la modificación de propague.
- El panel web de apps es muy limitado, es más rápido y se pueden hacer mas operaciones atacando las apis de Google apps.
- Google no da soporte de las apis, solo atiende consultas relativas al panel web de google apps.

Gracias

Más información, dudas…

Albert Vergés Ciurana
Albert.verges@udg.edu
Oriol Pellicer Sabrià
Oriol.pellicer@udg.edu

Servei Informàtic
Unitat de desenvolupament
de la universitat digital

Universitat de Girona