SERVICIO DE FIRMA DE DOCUMENTOS ALMACENADOS EN EL CLOUD (CLOUDDOCS)

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Luis Fernando Santocildes Romero

Profesor: Víctor García Font
Tutor: Juan Carlos Fernández Jara

Justificación y Contexto

- Desarrollo de las redes de comunicaciones de sistemas informáticos. Aumento de su uso desde los años 90.
- Entre 2019 y 2020, ha aumentado un 5% el total de ordenadores empresariales conectados a Internet.
- Aumento de ejecución de tareas y operaciones a distancia.
  - Compra-venta de bienes y servicios
  - Prestación de servicios
  - Firma de contratos, escrituras y otros documentos
  - Presentación de documentos y/o solicitudes firmadas ante empresas u otros organismos

La heterogeneidad de soluciones ha favorecido el anonimato.

- Delitos por suplantación de identidad
- Ciberacoso
- Fraudes en la compra-venta, sin que exista la posibilidad de reclamación

Justificación y Contexto

- **Soluciones Técnicas:**
  - *Técnicas de codificación de comunicaciones y documentos.*
  - *Mecanismos de identificación de usuarios.*
  - Certificados y Firma Electrónica.

- **Soluciones Jurídicas:**
  - *Leyes nacionales y transnacionales.*
  - ***Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 (eIDAS).***
    - **Regula la identificación y la firma electrónica.**
    - **Mejora de uso de los mismos.**
    - **Amplia legislaciones anteriores.**

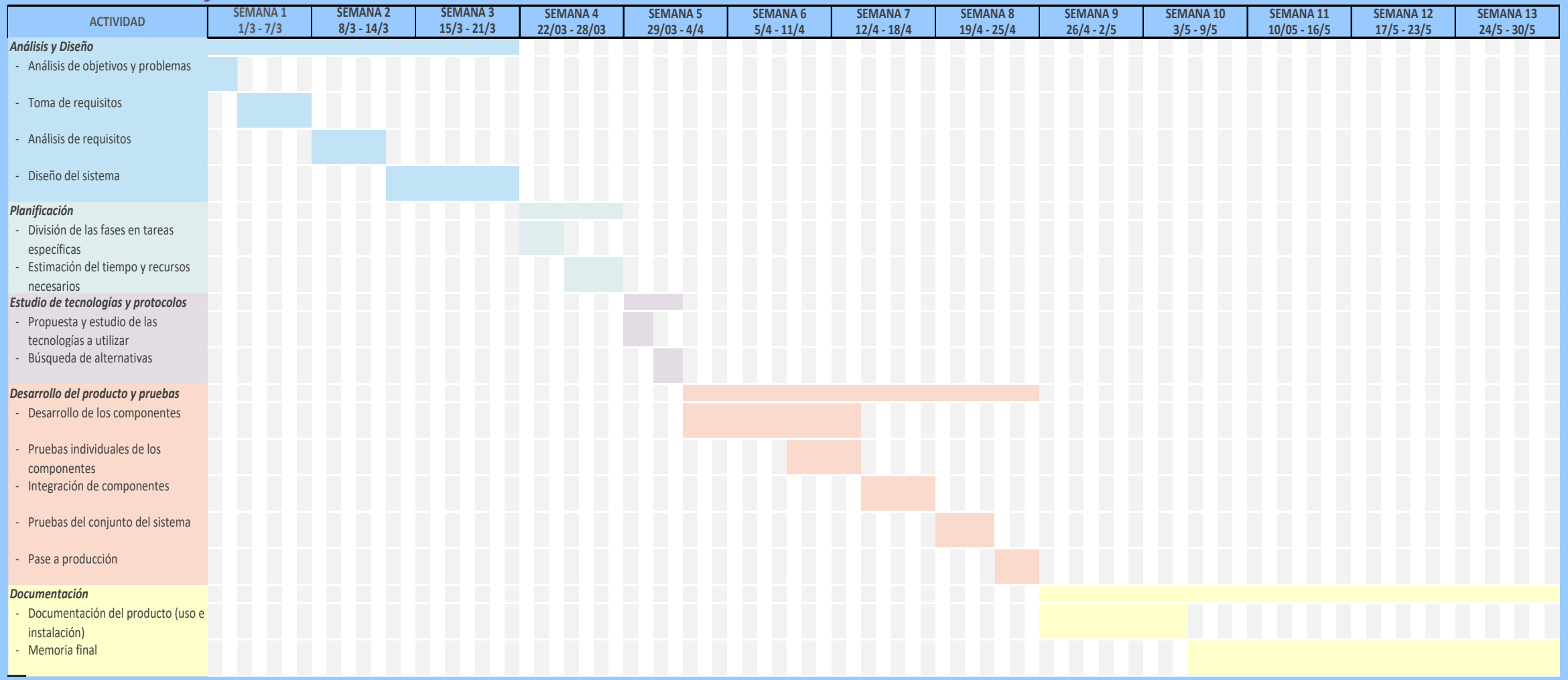
Objetivos

- Desarrollo de una aplicación para realizar la firma electrónica de documentos PDF.
  - *Cumplir con el reglamento eIDAS.*
  - *Usar arquitecturas, tecnologías y protocolos de comunicación estándares.*
  - *Simplicidad de uso.*
  - *Mantener el control del usuario sobre sus datos.*
  - *Existencia de una única versión.*

Metodología y Planificación

- División del trabajo en fases y etapas.

Plan de trabajo

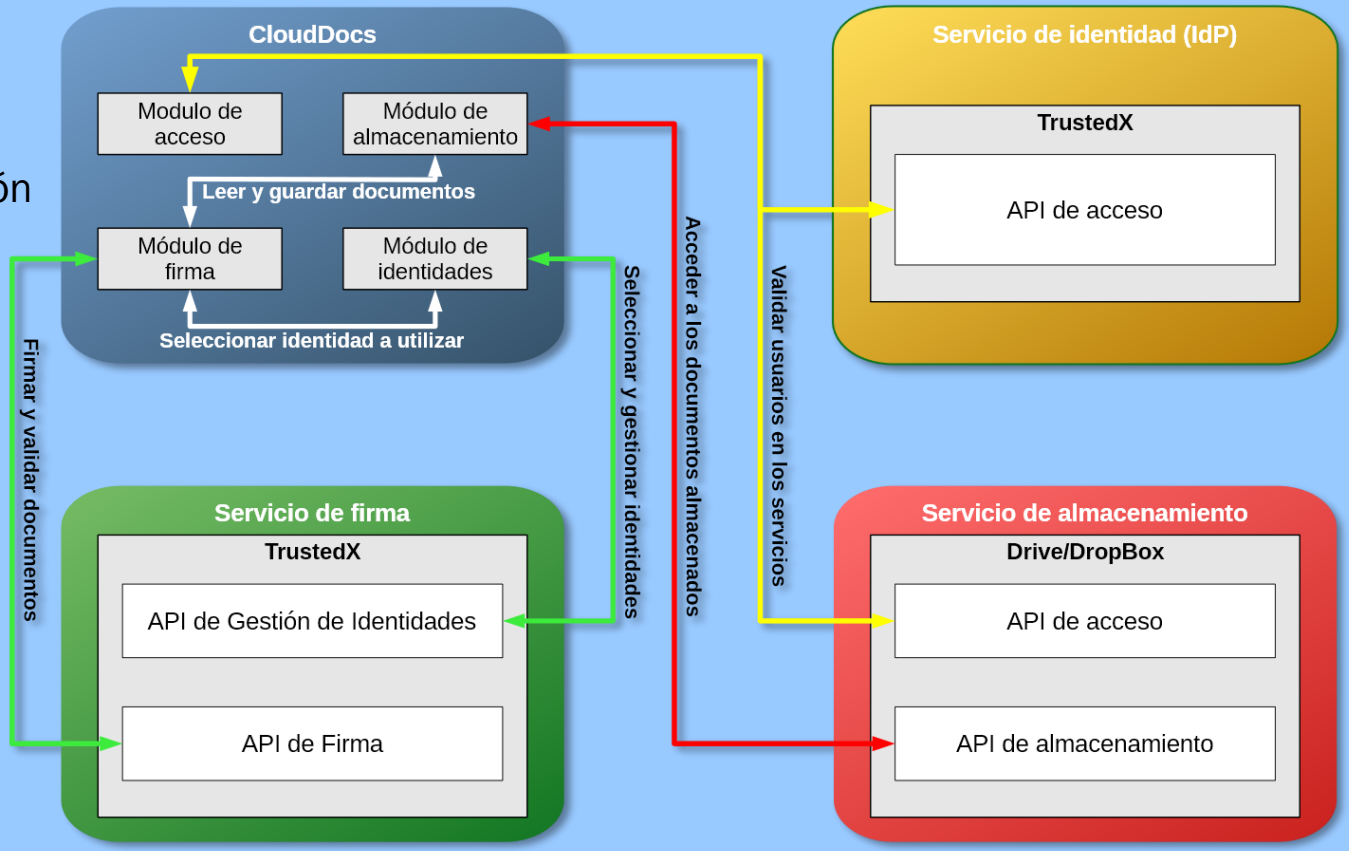


Arquitectura

Componentes principales

Núcleo de la aplicación:

- Principal
- Acceso/Autenticación
- Almacenamiento
- Firma
- Identidades



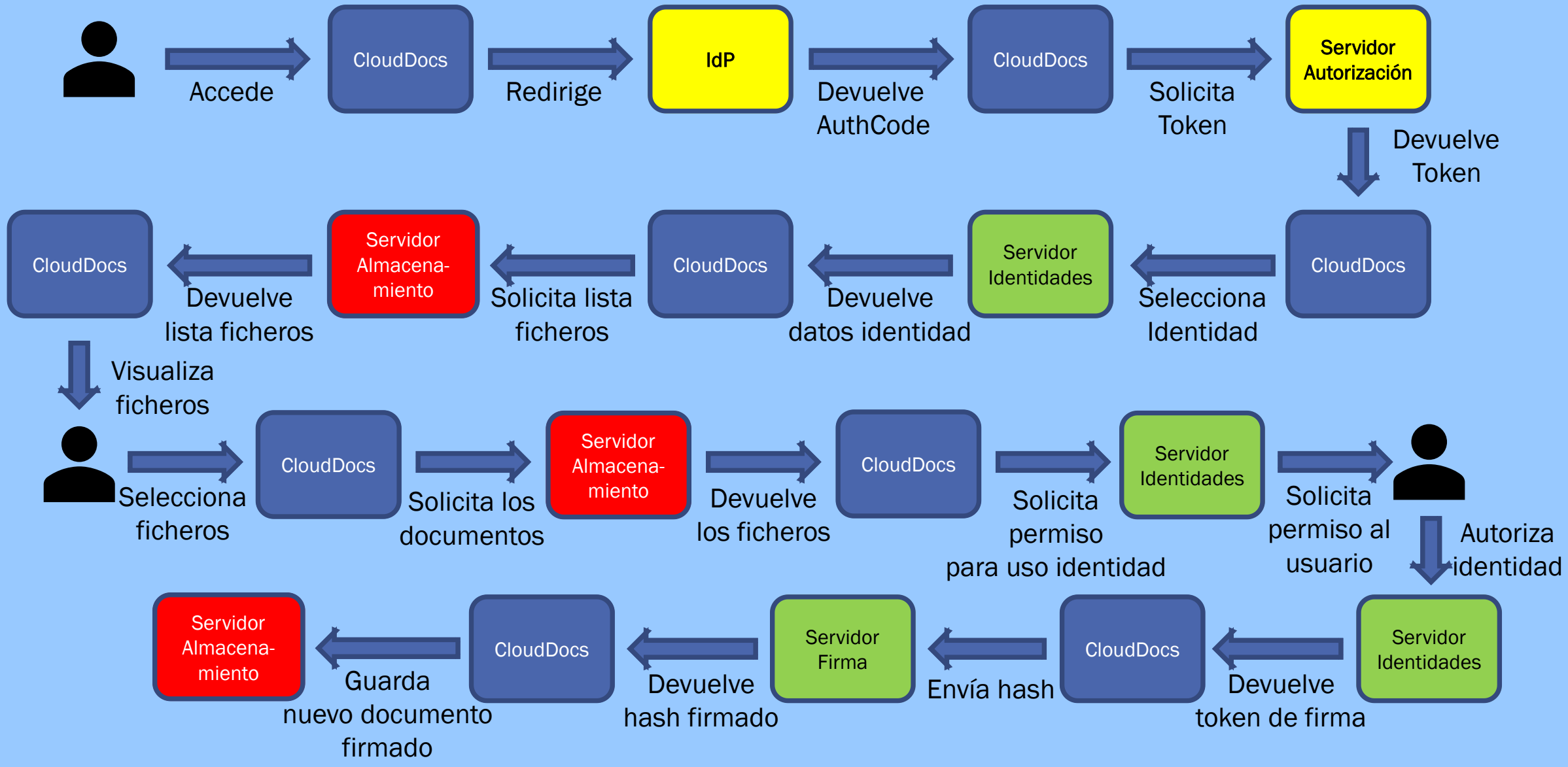
Servicios externos:

- Almacenamiento
  - Google Drive
  - Dropbox
- Firma / Identidad
  - TrustedX

Tecnologías:

- Java – Apache Tomcat
- Web – HTML/CSS/Javascript

Flujo de Firma



Consideraciones

- Demostrador
  - *Para cumplir* con el reglamento eIDAS es necesario:*
    - El servidor de identidades debe ser QSCD – **No PKCS#12**
    - El nivel de seguridad de identificación debe ser sustancial o algo – **2FA**

* Tarea pendiente de realizar como plan de mejora en futuro proyecto