Sistema Automatizado para la Firma y el Estampado Electrónico de Tiempo (Safet)

Antonio Araujo Brett[1] Víctor Bravo[1]

[1]Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres
Nodo Mérida

CENDITEL, 2008

Licencia de Uso

Agenda

1. **La automatización**
   - Definiciones y problemas
   - Flujo, Firmas electrónicas, Estampado de Tiempo
   - Revisión y uso
2. **SAFET**
   - El Proyecto
3. **Preguntas**

La automatización

Elemento Tecnológico: automatización de procesos

Inserción de la tecnología digital en el manejo de la información

Pero, qué problemas o aspectos ...

Aspectos o problemas ...

- Seguridad de la Información (Se verifica como último elemento)
- Desfase entre requisitos y las Características finales del software

Pero, qué problemas o aspectos ...

Aspectos o problemas ...

- Seguridad de la Información (Se verifica como último elemento)
- Desfase entre requisitos y las Características finales del software
- Cambio de relación de la comunidad con la tecnología

Pero, qué problemas o aspectos ...

Aspectos o problemas ...

- Seguridad de la Información (Se verifica como último elemento)
- Desfase entre requisitos y las Características finales del software
- Cambio de relación de la comunidad con la tecnología

Los elementos tecnológicos

Elemento tecnológico: Flujo de Trabajo

- Modela una secuencia de actividades vinculadas a documentos y personas
  - ¿Cuál será la mejor forma de organizarse?
  - ¿Existira puntos de flujo intenso o “cuellos de botellas”?

Los elementos tecnológicos

Elemento tecnológico: Flujo de Trabajo

- Modela una secuencia de actividades vinculadas a documentos y personas
  - ¿Cuál será la mejor forma de organizarse?
  - ¿Existira puntos de flujo intenso o “cuellos de botellas”?
  - ¿Cuál es el estado actual de la actividad?

Los elementos tecnológicos

Elemento tecnológico: Flujo de Trabajo

- Modela una secuencia de actividades vinculadas a documentos y personas
  - ¿Cuál será la mejor forma de organizarse?
  - ¿Existira puntos de flujo intenso o “cuellos de botellas”?
  - ¿Cuál es el estado actual de la actividad?
  - ¿Puedo inferir o detectar algunos comportamientos, según la historia?

Los elementos tecnológicos

Elemento tecnológico: Flujo de Trabajo

- Modela una secuencia de actividades vinculadas a documentos y personas
  - ¿Cuál será la mejor forma de organizarse?
  - ¿Existira puntos de flujo intenso o “cuellos de botellas”?
  - ¿Cuál es el estado actual de la actividad?
  - ¿Puedo inferir o detectar algunos comportamientos, según la historia?
  - ¿Puedo integrar datos de diferentes fuentes?

Los elementos tecnológicos

Elemento tecnológico: Flujo de Trabajo

- Modela una secuencia de actividades vinculadas a documentos y personas
  - ¿Cuál será la mejor forma de organizarse?
  - ¿Existira puntos de flujo intenso o “cuellos de botellas”?
  - ¿Cuál es el estado actual de la actividad?
  - ¿Puedo inferir o detectar algunos comportamientos, según la historia?
  - ¿Puedo integrar datos de diferentes fuentes?

Los elementos tecnológicos

Datos e Información...

La información es un elemento central en la automatización, ¿Cómo la percibimos? Usualmente...

Los elementos tecnológicos

Datos e Información...

La información es un elemento central en la automatización, ¿Cómo la percibimos? Usualmente...

Los elementos tecnológicos

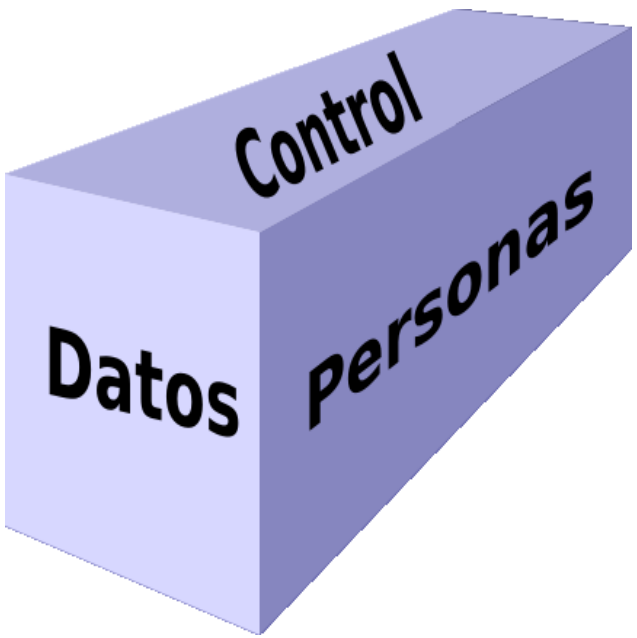
Datos e Información...

Podemos modelar utilizando tecnología y percibir la información de otras maneras: Por ejemplo...

Los elementos tecnológicos

Datos e Información...

Podemos modelar utilizando tecnología y percibir la información de otras maneras: Por ejemplo...



Los elementos tecnológicos

Perspectivas: ¿Cómo puedo ver la información?

- Control de flujo de Trabajo
- Datos / Documentos
- Roles / Usuarios Autorizados

Flujos de Trabajo

Modelo matemático del Flujo de Trabajo

- Lenguajes de “Negocios” orientado a SOA (BPEL,...)
- Basado en Patrones
- Basado en Redes de Petri (Petrinet)
- Modelo YAWL (Yet Another Workflow Language) $\Rightarrow$ PetriNet
- otros

Los elementos tecnológicos

Necesidad

Elemento tecnológico: **firma autógrafa**

- Identifica a la persona (1)
- Vincula a la persona con el acto jurídico (2)

Los elementos tecnológicos

Necesidad

Elemento tecnológico: **firma autógrafa**

- Identifica a la persona (1)
- Vincula a la persona con el acto jurídico (2)
- Utilizada en la realización de transacciones, operaciones, actividades (Vinculante)

Los elementos tecnológicos

Necesidad

Elemento tecnológico: **firma autógrafa**

- Identifica a la persona (1)
- Vincula a la persona con el acto jurídico (2)
- Utilizada en la realización de transacciones, operaciones, actividades (Vinculante)
- Verificación (Caracter biométrico)

Los elementos tecnológicos

Necesidad

Elemento tecnológico: **firma autógrafa**

- Identifica a la persona (1)
- Vincula a la persona con el acto jurídico (2)
- Utilizada en la realización de transacciones, operaciones, actividades (Vinculante)
- Verificación (Caracter biométrico)
- Culturalmente aceptado

Los elementos tecnológicos

Necesidad

Elemento tecnológico: **firma autógrafa**

- Identifica a la persona (1)
- Vincula a la persona con el acto jurídico (2)
- Utilizada en la realización de transacciones, operaciones, actividades (Vinculante)
- Verificación (Caracter biométrico)
- Culturalmente aceptado

Los elementos tecnológicos

Necesidad

Elemento tecnológico: **firma autógrafa**

- Identifica a la persona (1)
- Vincula a la persona con el acto jurídico (2)
- Utilizada en la realización de transacciones, operaciones, actividades (Vinculante)
- Verificación (Caracter biométrico)
- Culturalmente aceptado

Los elementos tecnológicos

Elemento tecnológico: **firma electrónica**

- Identifica a la persona (A un nivel aceptable p.e. tarjeta inteligente (1))
- Vincula a la persona con el acto jurídico (2) - En vía de... (p.e. Decreto/Reglamento Ley sobre Mensajes de Datos y Firmas Electrónicas.)

Los elementos tecnológicos

Elemento tecnológico: **firma electrónica**

- Identifica a la persona (A un nivel aceptable p.e. tarjeta inteligente (1))
- Vincula a la persona con el acto jurídico (2) - En vía de... (p.e. Decreto/Reglamento Ley sobre Mensajes de Datos y Firmas Electrónicas.)
- Objetivo de disminuir la carga al usuario

Los elementos tecnológicos

Elemento tecnológico: **firma electrónica**

- Identifica a la persona (A un nivel aceptable p.e. tarjeta inteligente (1))
- Vincula a la persona con el acto jurídico (2) - En vía de... (p.e. Decreto/Reglamento Ley sobre Mensajes de Datos y Firmas Electrónicas.)
- Objetivo de disminuir la carga al usuario
- Verificación (A un nivel aceptable p.e. tarjeta inteligente), pero en línea

Los elementos tecnológicos

Elemento tecnológico: **firma electrónica**

- Identifica a la persona (A un nivel aceptable p.e. tarjeta inteligente (1))
- Vincula a la persona con el acto jurídico (2) - En vía de... (p.e. Decreto/Reglamento Ley sobre Mensajes de Datos y Firmas Electrónicas.)
- Objetivo de disminuir la carga al usuario
- Verificación (A un nivel aceptable p.e. tarjeta inteligente), pero en línea

Los elementos tecnológicos

Elemento tecnológico: **firma electrónica**

- Identifica a la persona (A un nivel aceptable p.e. tarjeta inteligente (1))
- Vincula a la persona con el acto jurídico (2) - En vía de... (p.e. Decreto/Reglamento Ley sobre Mensajes de Datos y Firmas Electrónicas.)
- Objetivo de disminuir la carga al usuario
- Verificación (A un nivel aceptable p.e. tarjeta inteligente), pero en línea

Los elementos tecnológicos

Elemento tecnológico: **firma electrónica**

- Identifica a la persona (A un nivel aceptable p.e. tarjeta inteligente (1))
- Vincula a la persona con el acto jurídico (2) - En vía de... (p.e. Decreto/Reglamento Ley sobre Mensajes de Datos y Firmas Electrónicas.)
- Objetivo de disminuir la carga al usuario
- Verificación (A un nivel aceptable p.e. tarjeta inteligente), pero en línea

Comparación con la firma autógrafa

La firma electrónica es la autógrafa digitalizada?

NO

La firma electrónica es un método criptográfico que asegura la integridad del documento firmado así como la identidad del firmante.

01010101101 SÍ

Comparación con la firma autógrafa

Pregunta

¿La firma electrónica es legalmente equivalente a la firma autógrafa?

Comparación con la firma autógrafa

Pregunta

¿La firma electrónica es legalmente equivalente a la firma autógrafa?

Respuesta

Podría decirse que sí, pero debe estar validada por una Autoridad de Certificación (Tercero de confianza) que expida un certificado digital que diga que la firma es válida.

Firmar electrónicamente

- Resultado de aplicar cierto algoritmo matematico (función hash)
- Cuando la entrada es un documento, el resultado de la función (resena) es un número que identifica unívocamente al texto

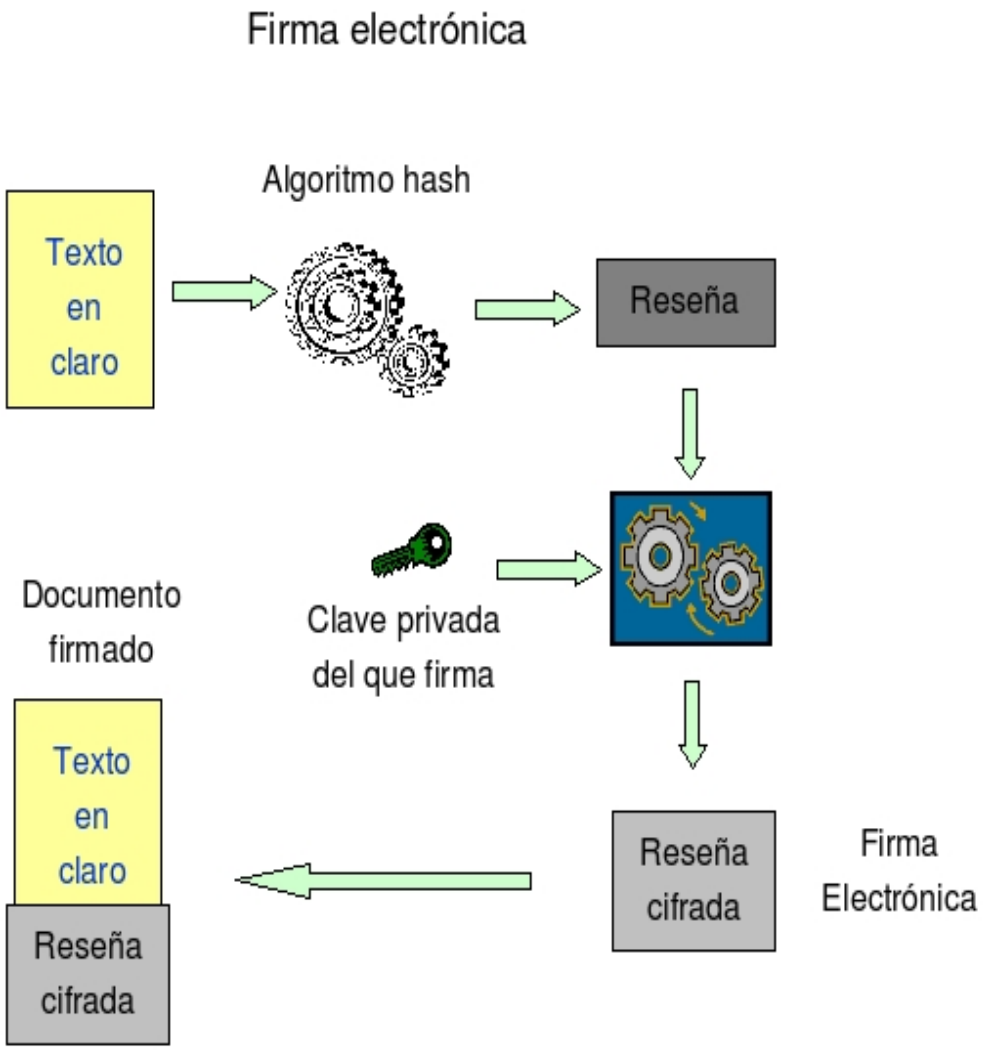
Firmar electrónicamente

- Resultado de aplicar cierto algoritmo matematico (función hash)
- Cuando la entrada es un documento, el resultado de la función (resena) es un número que identifica unívocamente al texto
- Se adjunta éste número al texto de manera cifrada con el algortimo asimétrico usando la clave privada del que firma.

Firmar electrónicamente

- Resultado de aplicar cierto algoritmo matematico (función hash)
- Cuando la entrada es un documento, el resultado de la función (resena) es un número que identifica unívocamente al texto
- Se adjunta éste número al texto de manera cifrada con el algortimo asimétrico usando la clave privada del que firma.

Firmar electrónicamente



Verificar firma electrónicamente

- El destinatario debe aplicar de nuevo la función hash al texto en claro y comparar su resultado (resena)
- se tiene que descifrar usando la clave pública del firmante

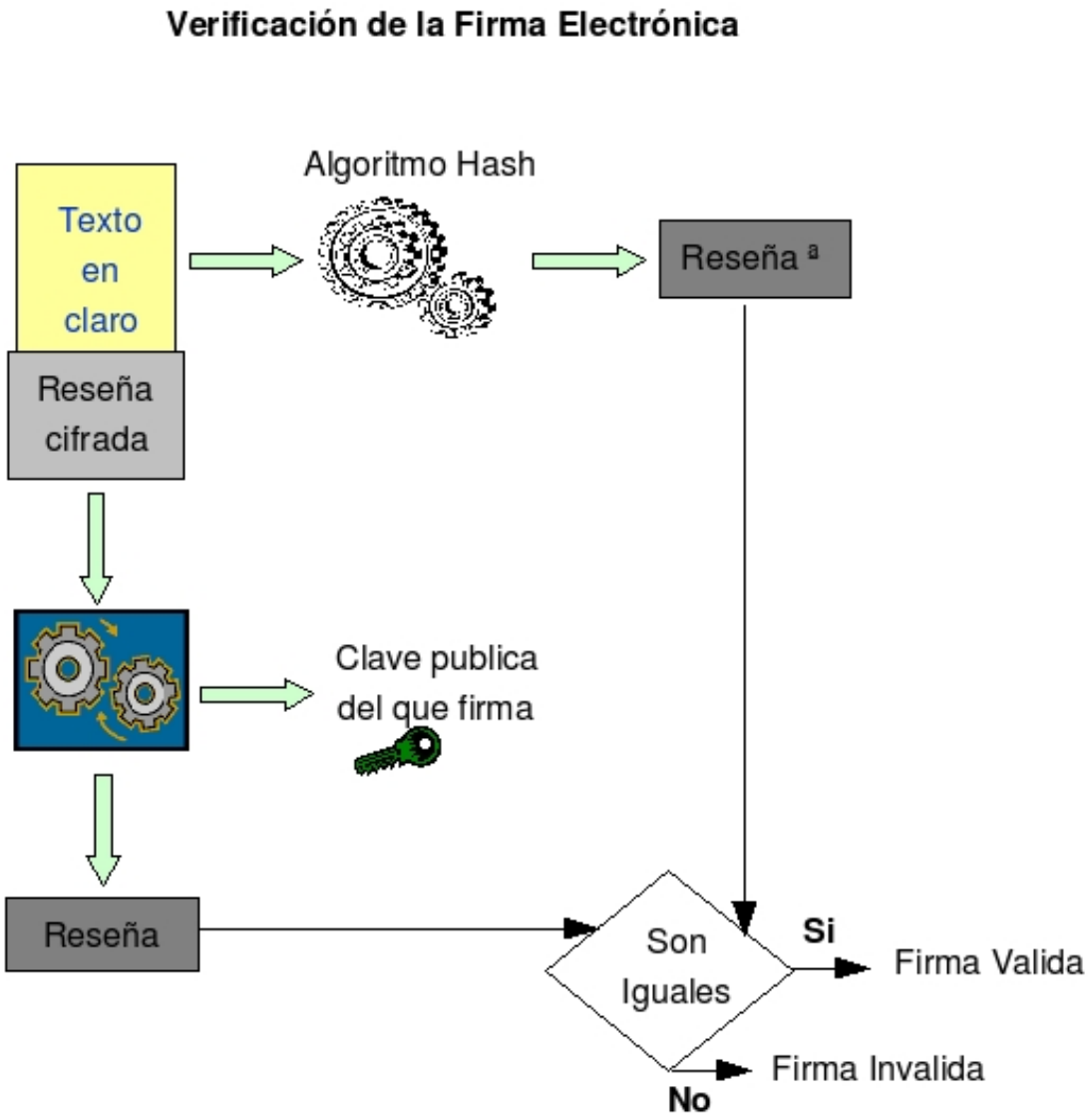
Verificar firma electrónicamente

- El destinatario debe aplicar de nuevo la función hash al texto en claro y comparar su resultado (resena)
- se tiene que descifrar usando la clave pública del firmante
- Si ambas son iguales: no fue modificado y aseguro identidad

Verificar firma electrónicamente

- El destinatario debe aplicar de nuevo la función hash al texto en claro y comparar su resultado (resena)
- se tiene que descifrar usando la clave pública del firmante
- Si ambas son iguales: no fue modificado y aseguro identidad

Verificar firma electrónicamente



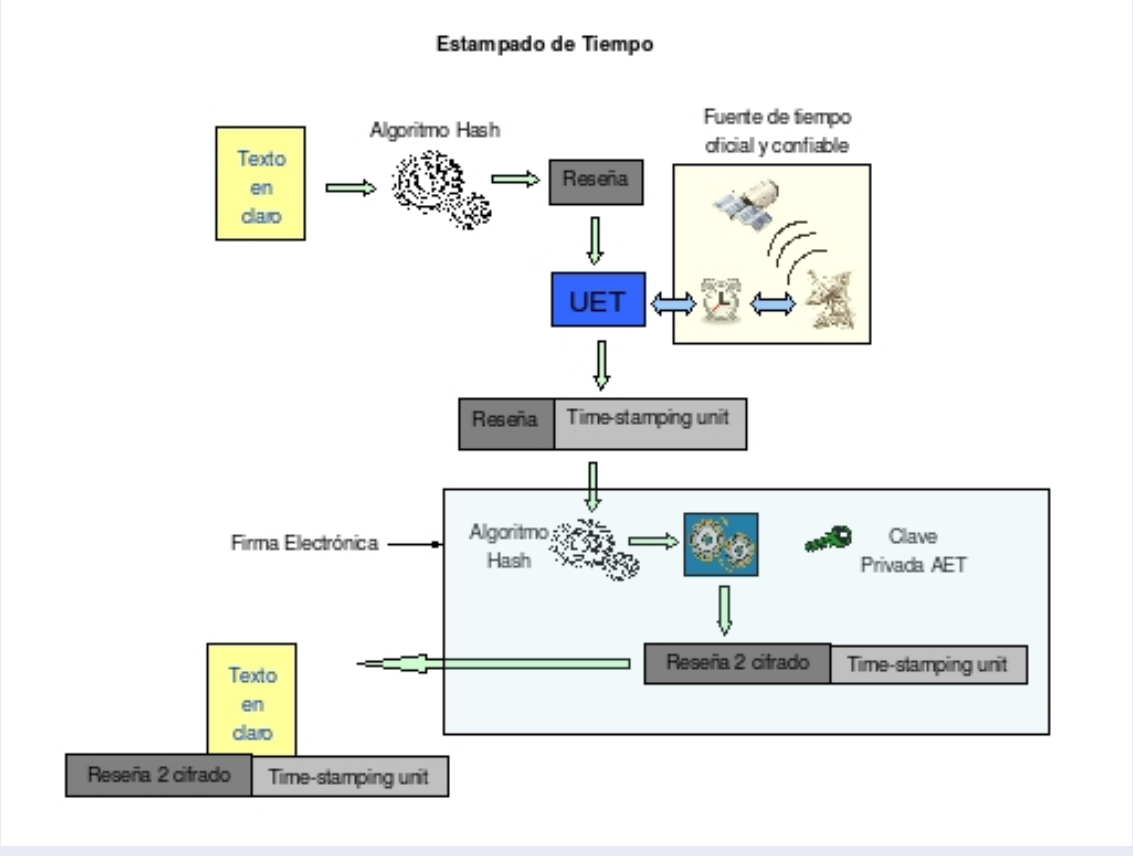
Estampado de Tiempo

Y si agregamos la hora/fecha ...

Si tenemos la suficiente confianza $\Longrightarrow$ Se certifica validez de datos digitales para determinado momento

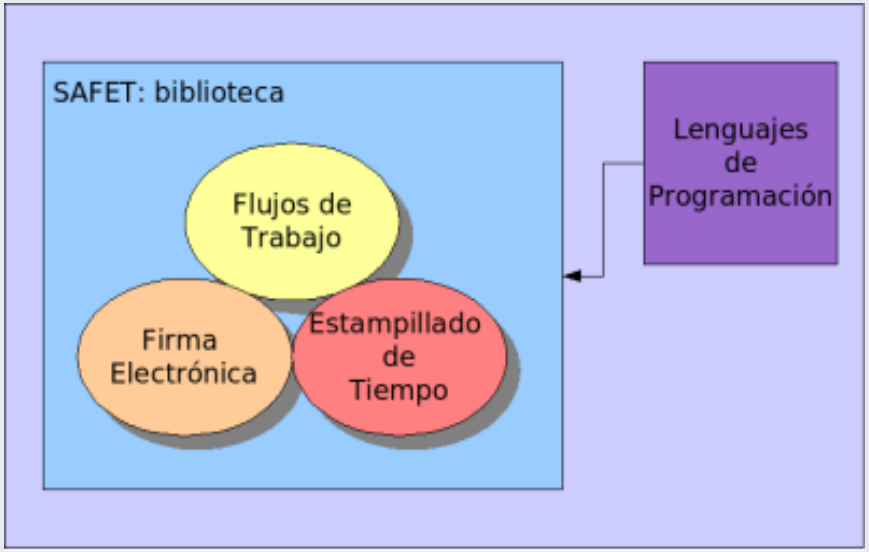
Estampado de Tiempo

¿Qué es el estampado de tiempo?



Descripción

Desarrollar una herramienta de software que permita la incorporación de las tecnologías de flujos de trabajo, firma electrónica y estampillado de tiempo en distintos sistemas de información.



Descripción

SAFET

- ***Flujos de trabajo*** apoyar la automatización de procesos
- ***Firma Electrónica*** expresar voluntad de aceptación en el mundo electrónico y establecer identidades virtuales
- ***Estampillado de Tiempo*** aplicar hora legal a documentos/transacciones electrónicas

Descripción

SAFET

Se pretende construir una Interfaz de Programación de Aplicaciones (API por sus siglas en inglés).

Características Generales

- Biblioteca de clases como núcleo de librería: ***libsafet***.
- Envoltorio para lenguajes de programación: inicialmente módulo PHP **libsafet-php**
- Utilización de dispositivos criptográficos para firmar electrónicamente documentos.
- Utilización de herramientas y tecnologías libres.

Herramientas utilizadas para la construcción

Lenguaje de programación C++

- Lenguaje nativo de desarrollo para la librería ***libsafet***

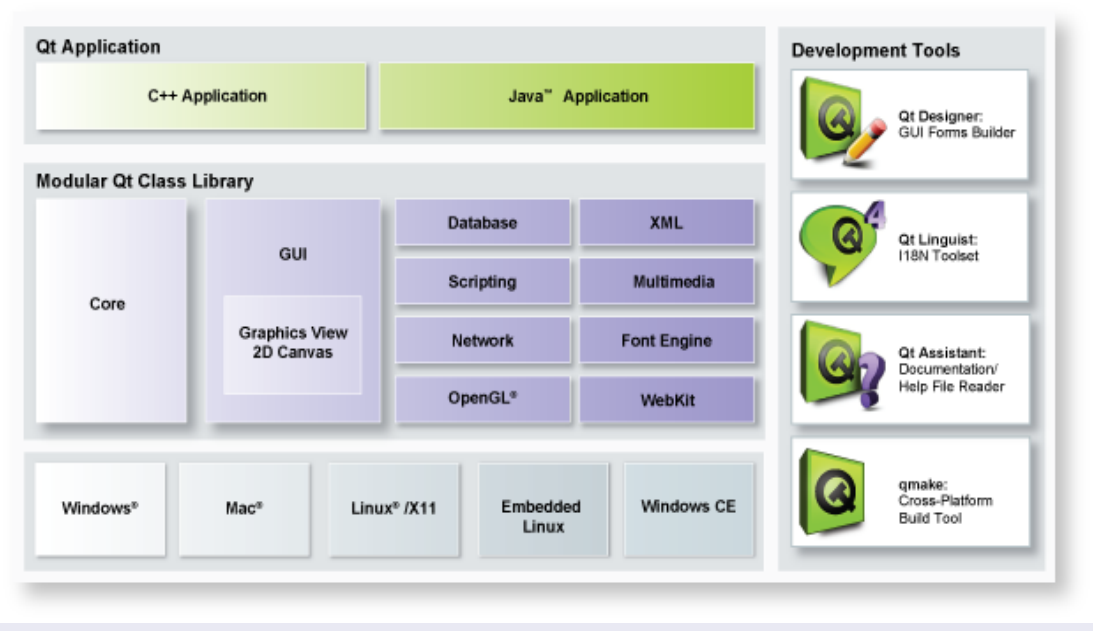
Lenguaje de programación PHP

- Lenguaje de desarrollo para envoltorio de la librería en forma de módulo PHP: ***libsafet-php***
- Herramientas utilitarias para generación de módulo.

Herramientas utilizadas para la construcción

Framework de desarrollo Qt

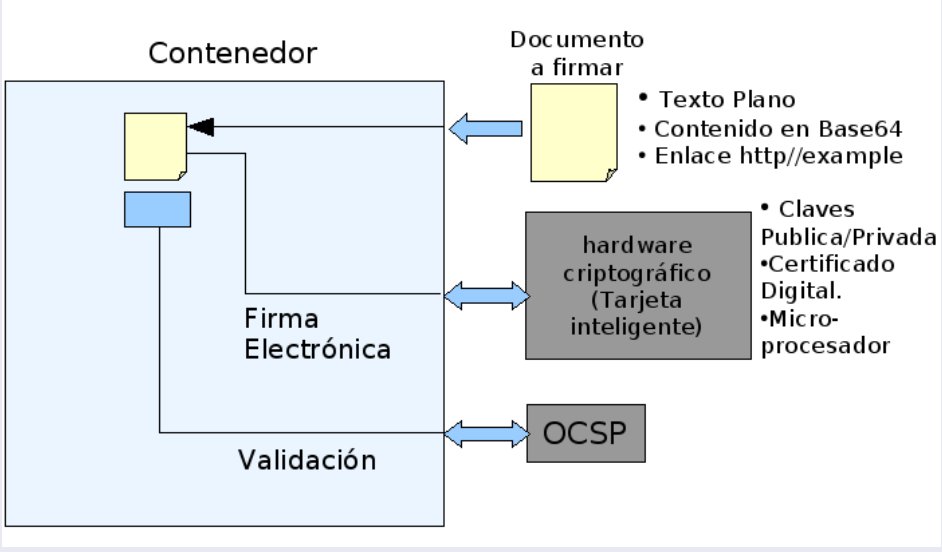
- Framework de desarrollo de aplicaciones
- API intuitiva y amplia librería de clases C++
- *http://trolltech.com/products/qt/*



Herramientas utilizadas para la construcción

Librería Libdigidoc

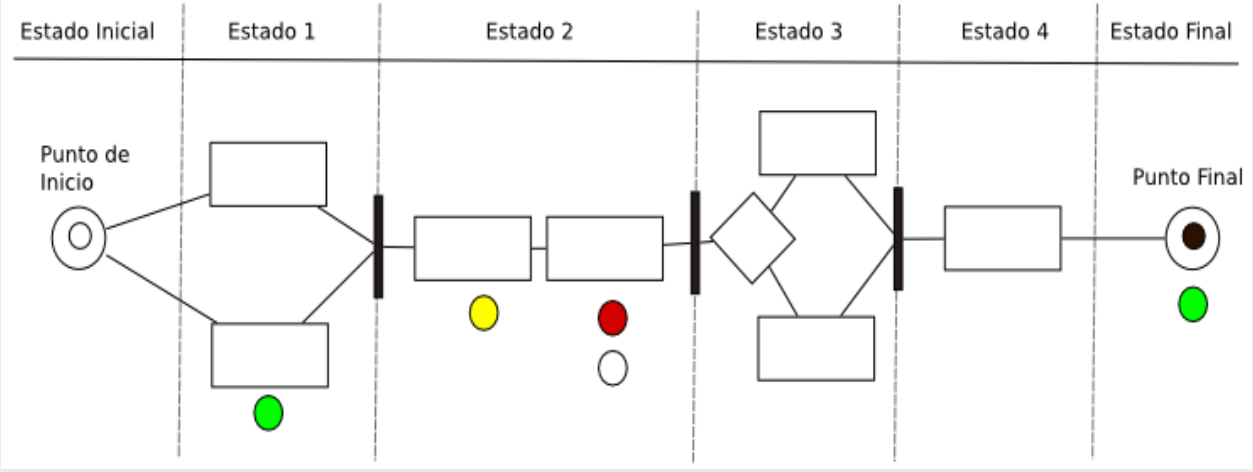
- Implementación del estándar XAdES (XML Advanced Electronic Signature) del proyecto OpenXAdES (*http://www.openxades.org*).
- Creación de un formato común para documentos con firma electrónica y estampillado de tiempo (XML).



Herramientas utilizadas para la construcción

Lenguaje YAWL - Yet Another Workflow Language

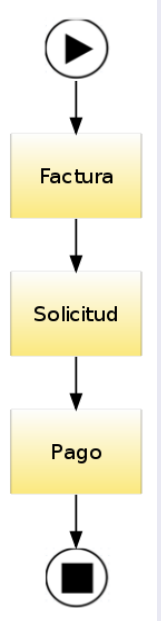
- Utilizado para el modelado y gestión de flujos de trabajo
- *http://www.yawl-system.com*



Herramientas utilizadas para la construcción

Librería Graphviz

- Utilizada para dibujar grafos asociados a flujos de trabajo
- *http://www.graphviz.org*



Herramientas utilizadas para la construcción

Librería dbxml

- Base de datos diseñada para almacenamiento y recuperación de documentos en formato XML.
- Almacen de documentos firmados electrónicamente.

Herramientas utilizadas para la construcción

Conexión con base de datos relacional

- Uso de driver para mantener la transparencia con repositorios relacionales.
- Pruebas con base de datos Postgresql *http://www.postgresql.org*

Características Funcionales Generales

Flujo de Trabajo

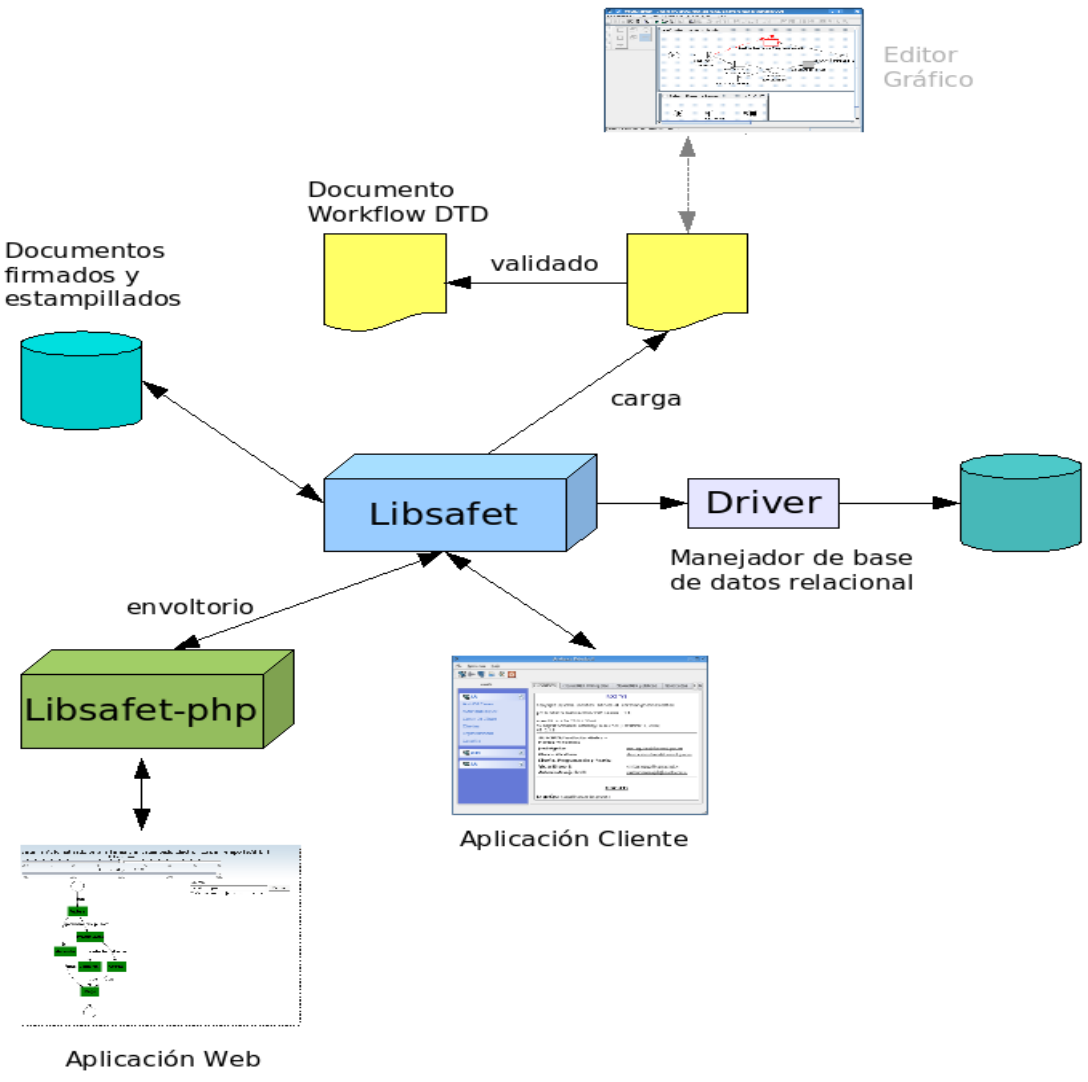
- Crear documento
- Modificar documento
- Definir actividades, reglas y condiciones de un flujo
- Visualizar documento
- Chequear estadísticas

Características Funcionales Generales

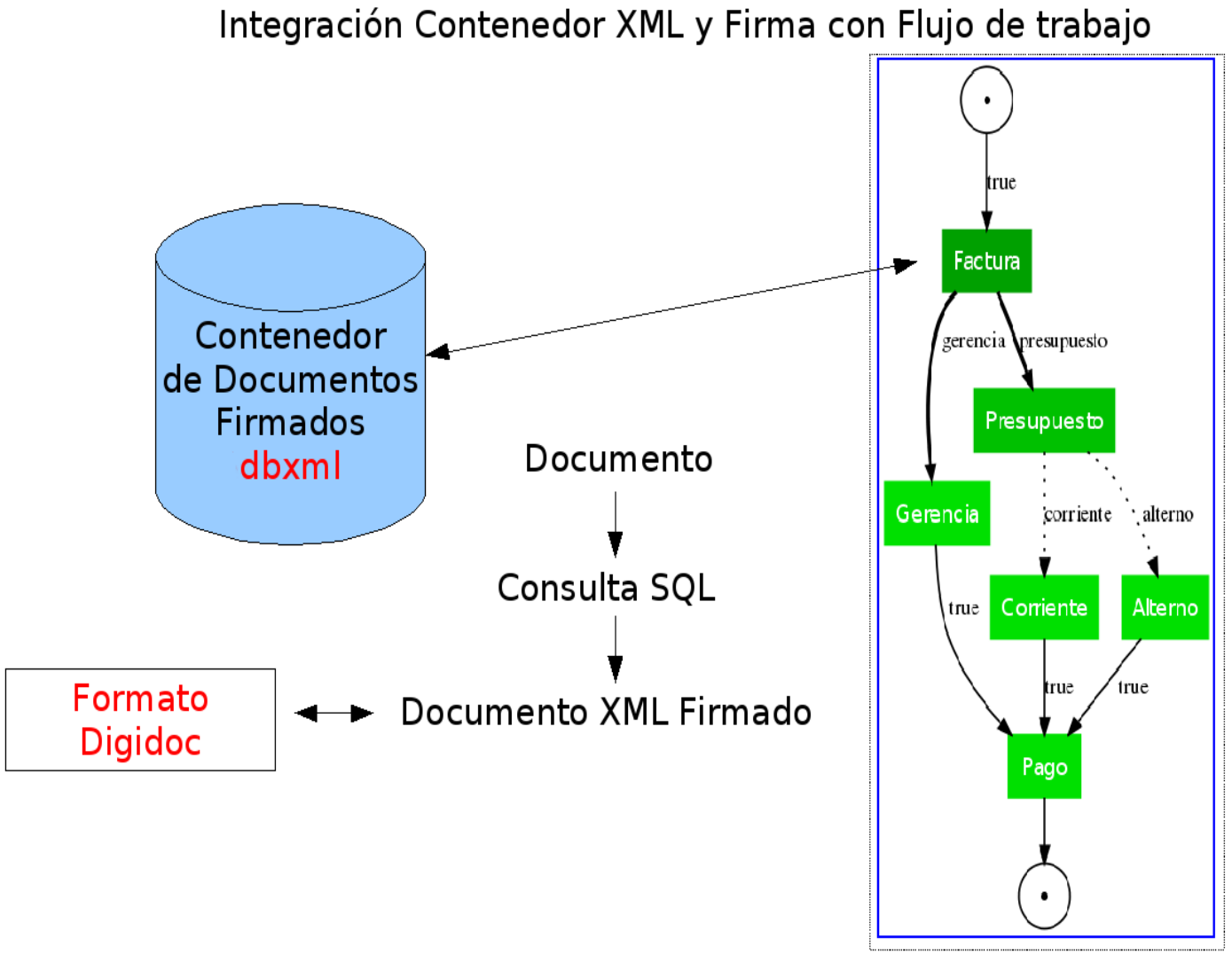
Firma Electrónica y Estampillado de Tiempo

- Gestión de contenedores (crear, modificar, eliminar)
- Aplicar firma electrónica con dispositivo criptográfico
- Verificar firma electrónica
- Aplicar estampillado de tiempo
- Verificar estampillado de tiempo

Arquitectura General del sistema



Biblioteca Libsafet



Biblioteca Libsafet

Modelado de Flujo de Trabajos

- Cálculo de documentos: estadísticas y situación actual de un flujo.
- Disponibilidad de operadores para determinar qué documentos se encuentran en determinada actividad/tarea

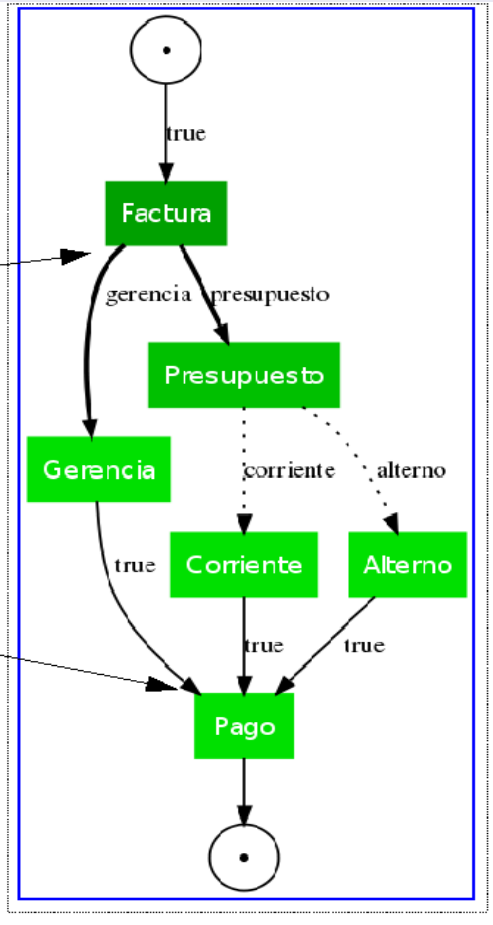
Biblioteca Libsafet

Modelado de Flujo de Trabajos

Cálculo de documentos:

Operadores:

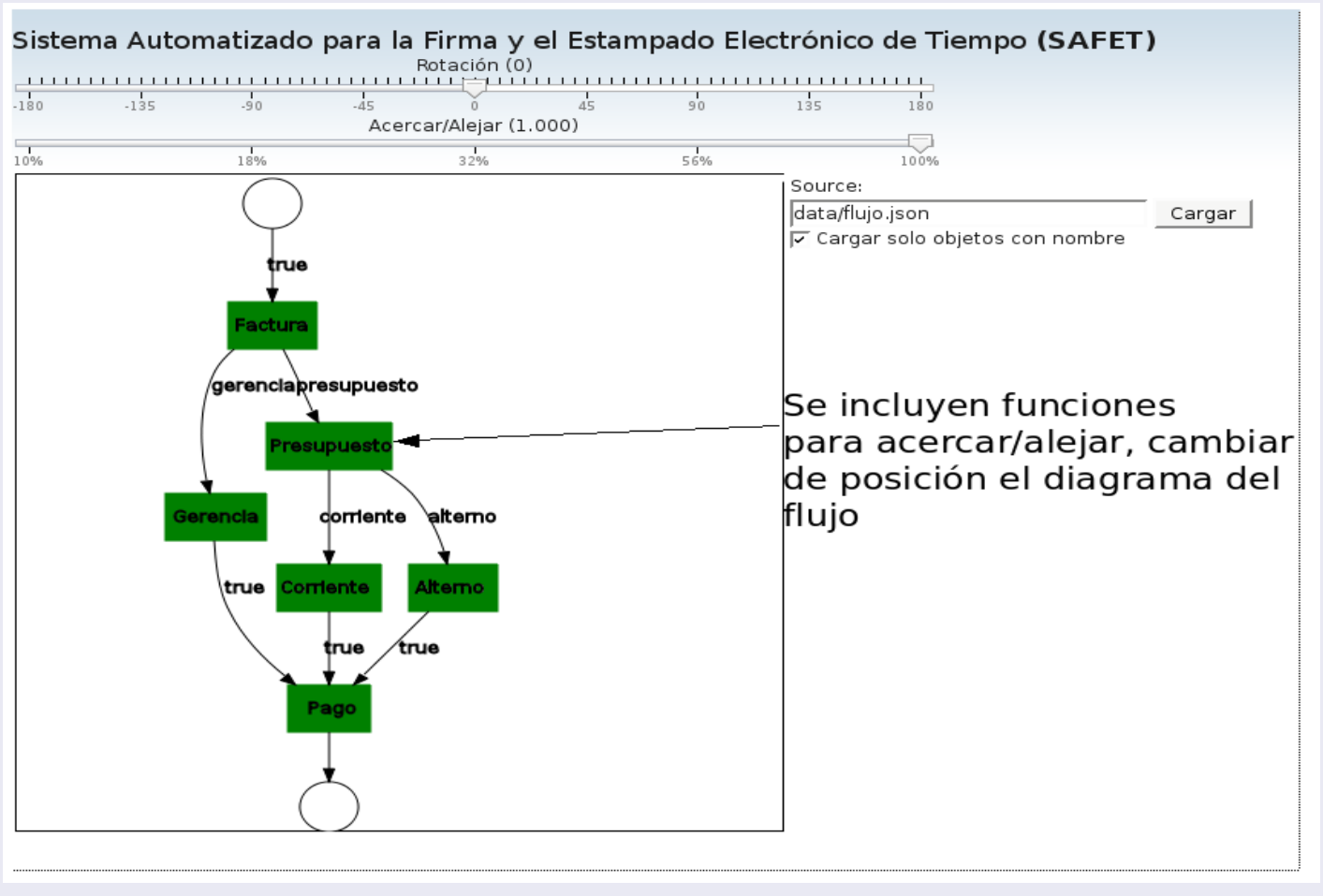
SPLIT-AND
SPLIT-OR
SPLIT-XOR
SPLIT-2-OUT-3
JOIN-AND
JOIN-OR
JOIN-XOR
JOIN-2-OUT-3



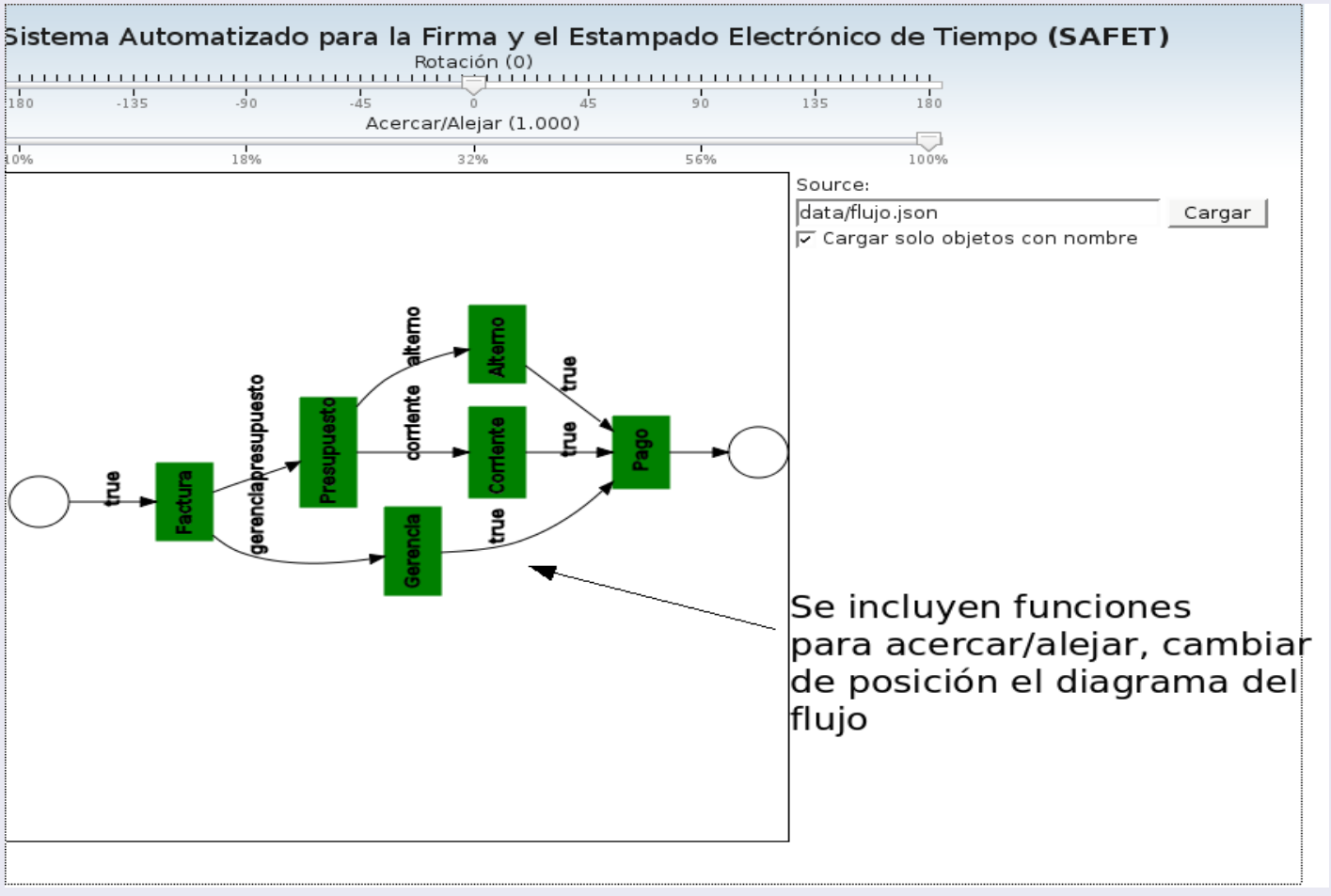
Módulo PHP Libsafet-php

- Estudio de distintas tecnologías y herramientas gráficas para desarrollar funciones de despliegue de **libsafet-php**.
- Uso de AJAX (a través de la librería Dojotoolkit para una aplicación demo).
- Uso del formato JSON (parecido a XML, pero para uso de JavaScript y consultas parecidas a una Arquitectura basada en Servicios).
- Construcción de un programa de ejemplo

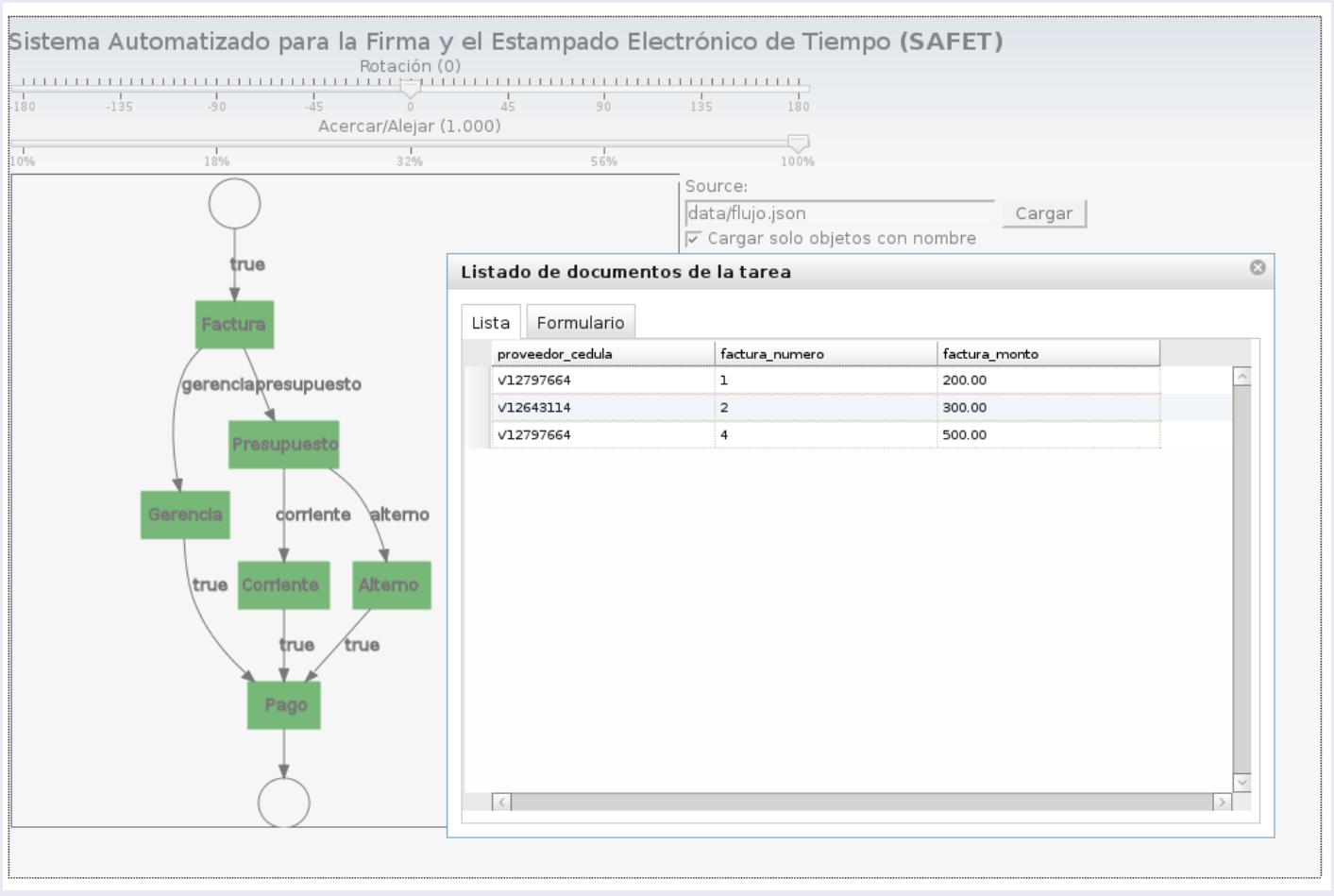
Módulo PHP Libsafet-php



Módulo PHP Libsafet-php



Módulo PHP Libsafet-php



Desarrollo

- Para el desarrollo del proyecto SAFET se sigue la Metodología de Desarrollo de Software Libre [1].
- Se planificaron 3 iteraciones para completar el desarrollo.
- Actualmente se está trabajando en la 2da iteración del desarrollo.

[1] http://wiki.cenditel.gob.ve/metodologia

Desarrollo

Al finalizar las 3 iteraciones del desarrollo se espera tener como producto final:

- Un programa basado en consola que provea las funcionalidades de SAFET
- Un envoltorio del sistema SAFET para el lenguaje PHP en forma de módulo.
- Demo, tutoriales.
- Funciones para páginas predefinidas.
- Documentación de usuario y de programador.

Posibles aplicaciones de SAFET

- Sistemas web
- Sistemas administrativos
- Sistemas de gestión de documentos
- Entre otros

Vinculación con:

- Iniciativas y proyectos en el marco de la Infraestructura Nacional de Certificación Electrónica supervisada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).
- Proyecto Cédula Electrónica adelantado por la Oficina Nacional de Identificación y Extranjería (ONIDEX).
- entre otros.

Recursos del proyecto y trabajo colaborativo

Toda la información relacionada con el proyecto se encuentra alojada en la fábrica de software libre y la página del proyecto:

- `http://fsl.cenditel.gob.ve/safet`
- `http://repositorio.cenditel.gob.ve/safet`

Consultas adicionales: `seguridad@cenditel.gob.ve`

Preguntas, Dudas y Comentarios

≪ Inteligencia es lo que usas cuando no sabes qué hacer.≫

Jean Piaget