



SISTEMA DE FIRMA DIGITAL PARA EL MINISTERIO DE OBRAS PÚBLICAS, SERVICIOS Y VIVIENDA

Armin Mesa Sanchez

Tutor: Msc. Aldo Ramiro Valdez Alvarado
Asesor: Lic. Freddy Miguel Toledo Paz

ÍNDICE

1. MARCO INTRODUCTORIO
2. MARCO TEÓRICO
3. MARCO APLICATIVO
4. CALIDAD Y SEGURIDAD
5. ANÁLISIS COSTO BENEFICIO
6. CONCLUSIONES Y RECOMENDACIONES
7. DEMOSTRACIÓN

ÍNDICE

1. MARCO INTRODUCTORIO

1.INTRODUCCIÓN

2.ANTECEDENTES

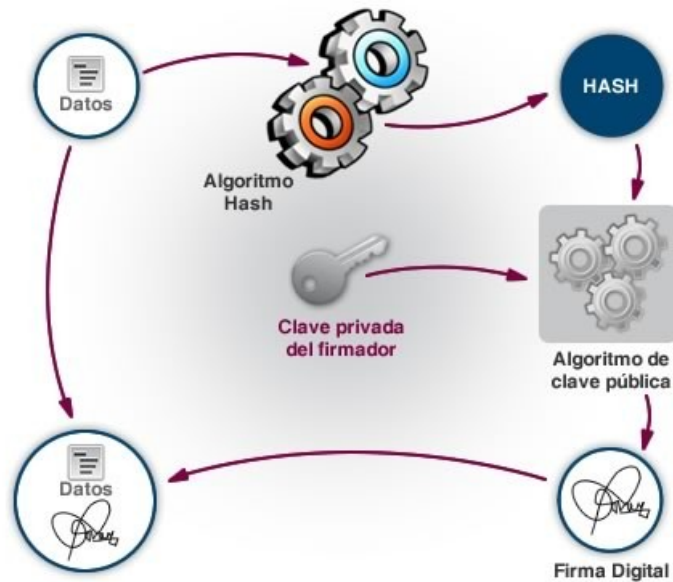
3.PROBLEMA CENTRAL

4.OBJETIVO GENERAL

5.ALCANCES Y LÍMITES

6.APORTES

INTRODUCCIÓN



- Ley 164 (Capítulo 3)
- Decreto Supremo 1793
- Resolución Administrativa regulatoria ATT-DJ-RA TL LP 32/2015



ÍNDICE

1. MARCO INTRODUCTORIO

1.INTRODUCCIÓN

2.ANTECEDENTES

3.PROBLEMA CENTRAL

4.OBJETIVO GENERAL

5.ALCANCES Y LÍMITES

6.APORTES

ANTECEDENTES



ÍNDICE

1. MARCO INTRODUCTORIO

1.INTRODUCCIÓN

2.ANTECEDENTES

3.PROBLEMA CENTRAL

4.OBJETIVO GENERAL

5.ALCANCES Y LÍMITES

6.APORTES

PROBLEMA CENTRAL

¿De que manera se puede agilizar, transparentar y simplificar los procedimientos administrativos de la gestión pública del Ministerio de Obras Públicas, Servicios y Vivienda?



ÍNDICE

1. MARCO INTRODUCTORIO

1.INTRODUCCIÓN

2.ANTECEDENTES

3.PROBLEMA CENTRAL

4.OBJETIVO GENERAL

5.ALCANCES Y LÍMITES

6.APORTES

OBJETIVO GENERAL

Desarrollar e implementar un sistema de firma digital para el Ministerio de Obras Públicas, Servicios y Vivienda que permita agilizar, transparentar y simplificar los procedimientos administrativos de la gestión pública.



ÍNDICE

1. MARCO INTRODUCTORIO

1.INTRODUCCIÓN

2.ANTECEDENTES

3.PROBLEMA CENTRAL

4.OBJETIVO GENERAL

5.ALCANCES Y LÍMITES

6.APORTES

ALCANCES Y LIMITES

Módulos a implementar



- Módulo vista PDF y marca de agua
- Módulo acceso Token, Fichero de claves
- Módulo para firmar
- Módulo de validación
- Módulo para sello de tiempo

No se contempla



- No asegurar seguridad para usuario
- Uso inadecuado de usuario
- Perduración de firma digital
- Sistema no Web
- Certificación de Software

ÍNDICE

1. MARCO INTRODUCTORIO

1.INTRODUCCIÓN

2.ANTECEDENTES

3.PROBLEMA CENTRAL

4.OBJETIVO GENERAL

5.ALCANCES Y LÍMITES

6.APORTES

APORTES

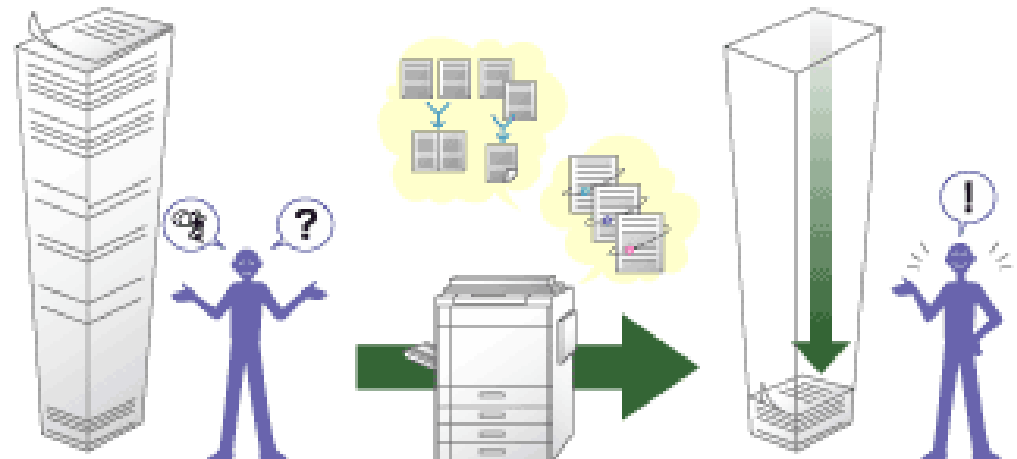
Sistemas eficientes y ágiles



Presencia física no necesaria



Reducción considerable de papel



ÍNDICE

1. MARCO INTRODUCTORIO

2. MARCO TEÓRICO

1. CRIPTOGRAFÍA

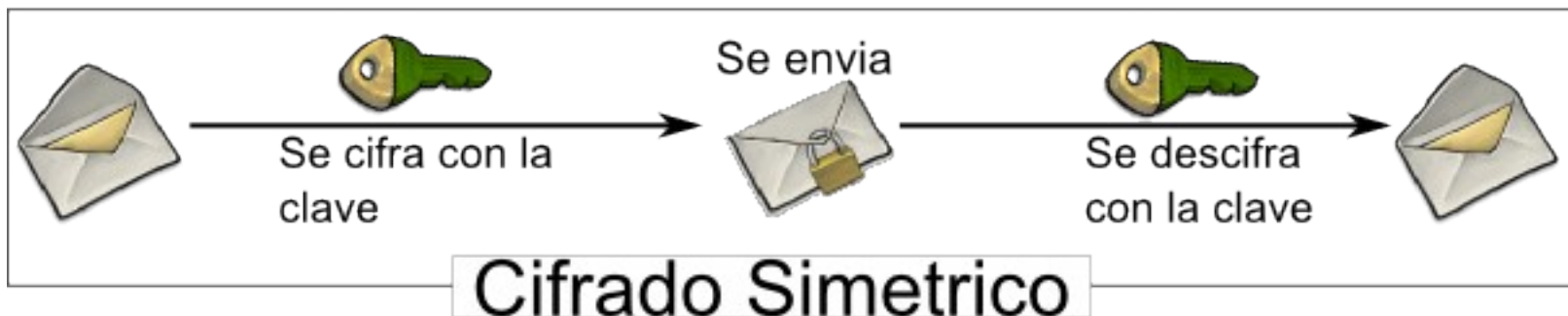
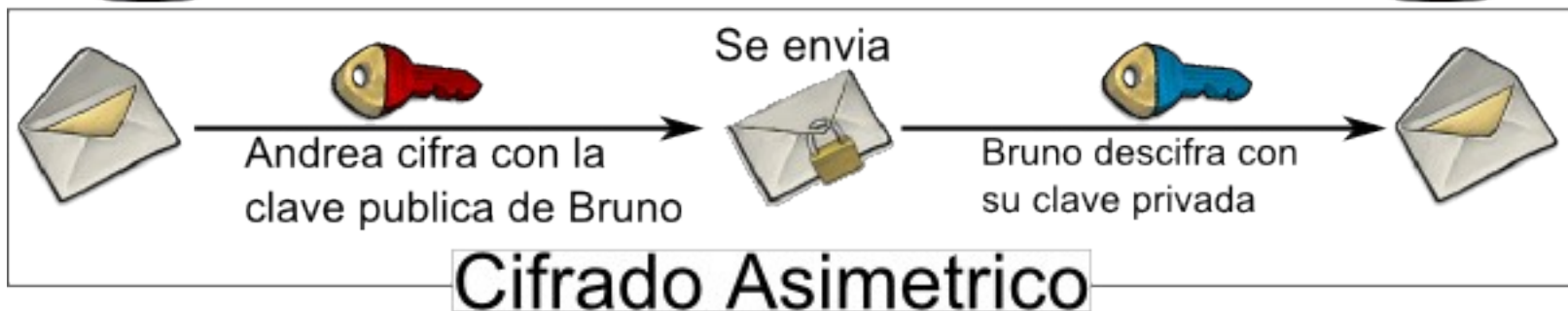
2. CERTIFICADO DIGITAL

3. REVOCACIÓN DE CERTIFICADOS

4. FIRMA DIGITAL

5. METODOLOGÍA DE DESARROLLO

CRIPTOGRAFÍA



RSA (Rivest, Shamir y Adleman) de 2048 Bits – RFC 5280

ÍNDICE

1. MARCO INTRODUCTORIO

2. MARCO TEÓRICO

1. CRIPTOGRAFÍA

2. CERTIFICADO DIGITAL

3. REVOCACIÓN DE CERTIFICADOS

4. FIRMA DIGITAL

5. METODOLOGÍA DE DESARROLLO

CERTIFICADO DIGITAL

- **Certificado de Autoridad**
- Certificado de Servidor
- **Certificado Personal**
- Certificado de productos de software (X.509 – RFC 2650)

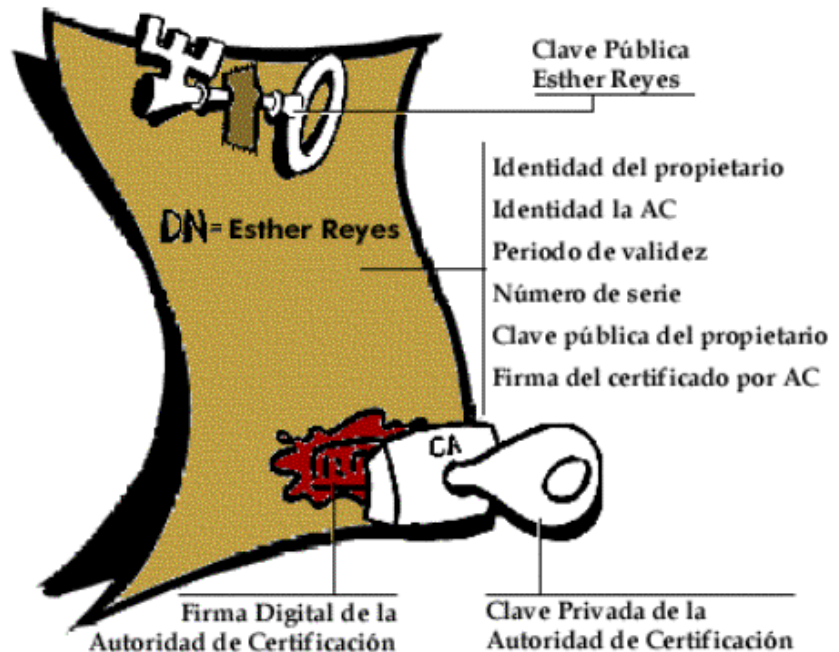


Policy Certification Authorities (PCA)



Certification Authorities (CA)

(RFC - 1422)



Propiedades

- Autenticación
- Confidencialidad
- Integridad
- Privacidad
- No repudio

ÍNDICE

1. MARCO INTRODUCTORIO

2. MARCO TEÓRICO

1. CRIPTOGRAFÍA

2. CERTIFICADO DIGITAL

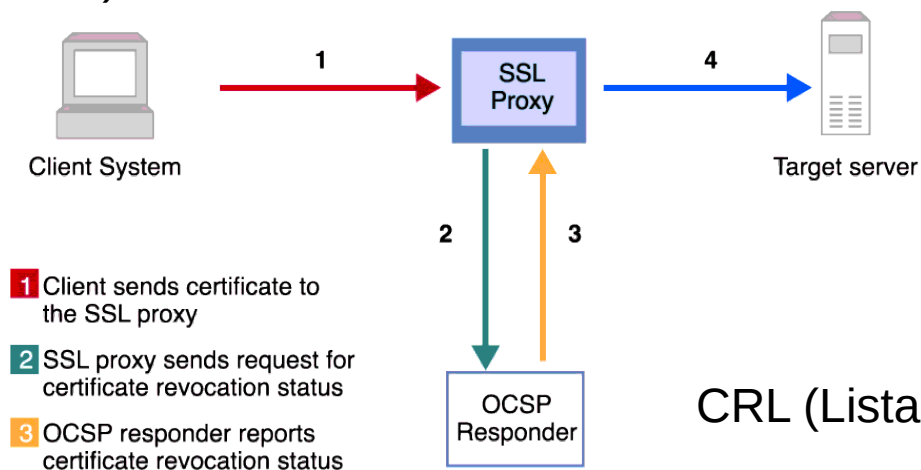
3. REVOCACIÓN DE CERTIFICADOS

4. FIRMA DIGITAL

5. METODOLOGÍA DE DESARROLLO

REVOCACIÓN DE CERTIFICADOS

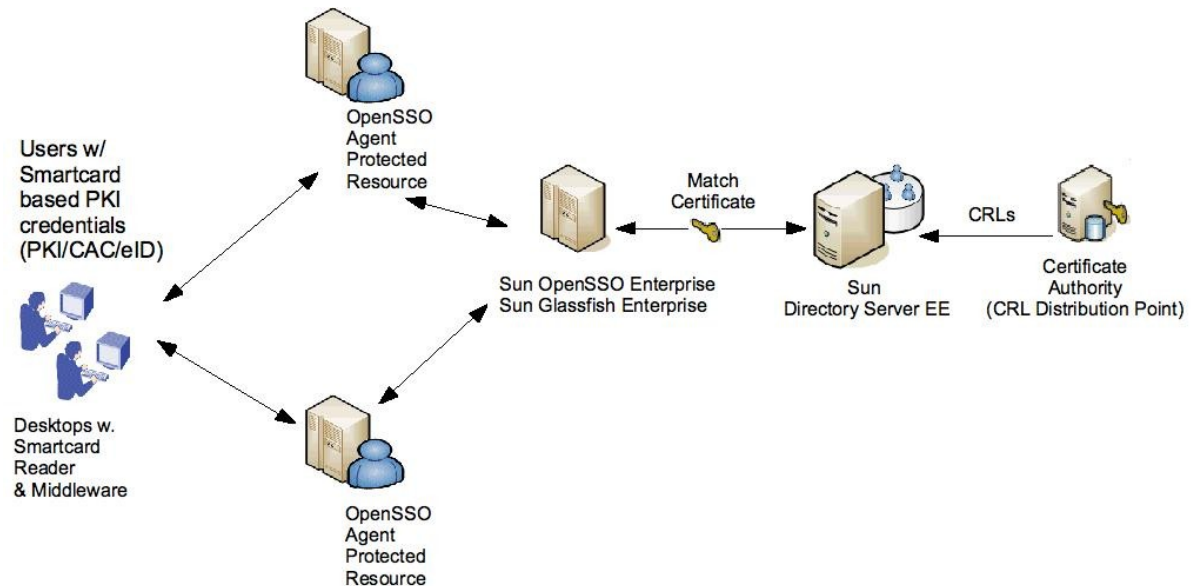
OCSP (Protocolo de Estado de Certificado en Línea) – RFC 2560



TSA (Sellado de Tiempo) – RFC 3161



CRL (Lista de Revocación de Certificado – RFC 3280)



ÍNDICE

1. MARCO INTRODUCTORIO

2. MARCO TEÓRICO

1. CRIPTOGRAFÍA

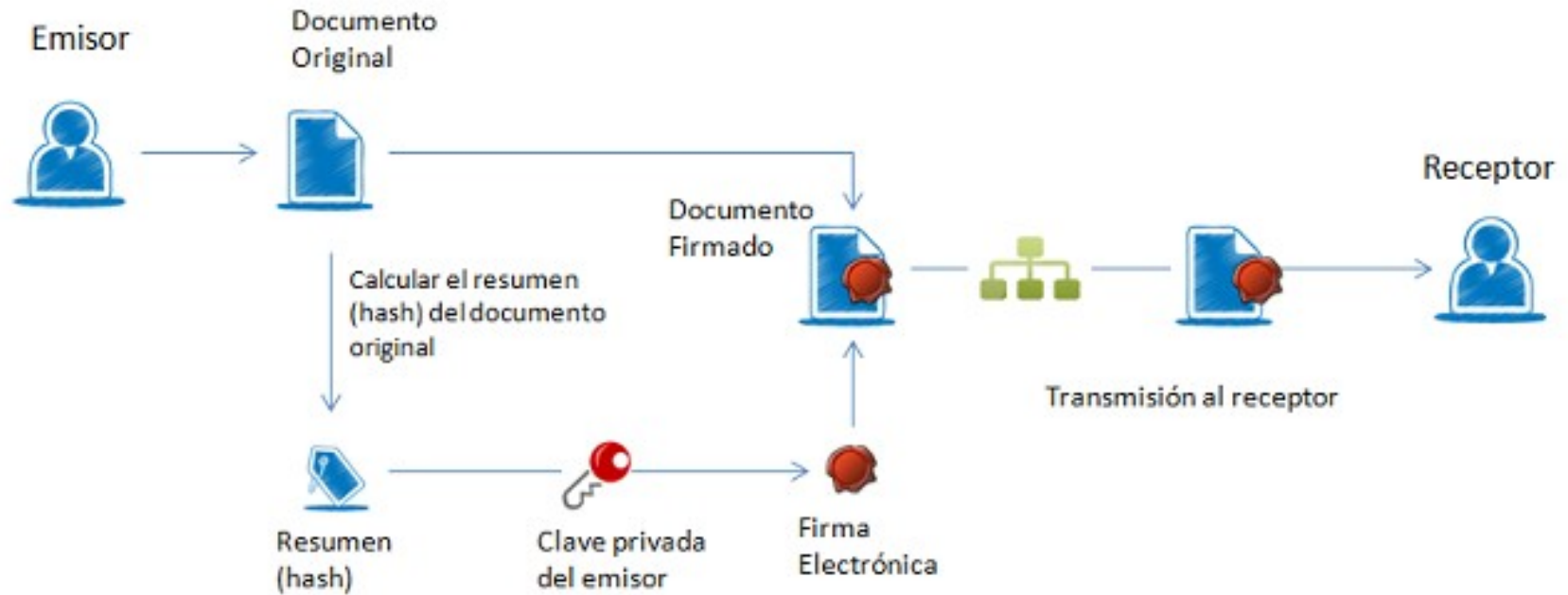
2. CERTIFICADO DIGITAL

3. REVOCACIÓN DE CERTIFICADOS

4. FIRMA DIGITAL

5. METODOLOGÍA DE DESARROLLO

FIRMA DIGITAL



- SHA -1 (Algoritmo Hash Seguro) 160 Bits – RFC 3174
- SHA – 256 (Algoritmo Hash Seguro) 256 Bits

PKCS#7 (Estándar de Criptografía de Clave Pública) – RFC 2315

PKCS#11 - RFC 7512

PKCS#12 – RFC 7292

ÍNDICE

1. MARCO INTRODUCTORIO

2. MARCO TEÓRICO

1. CRIPTOGRAFÍA

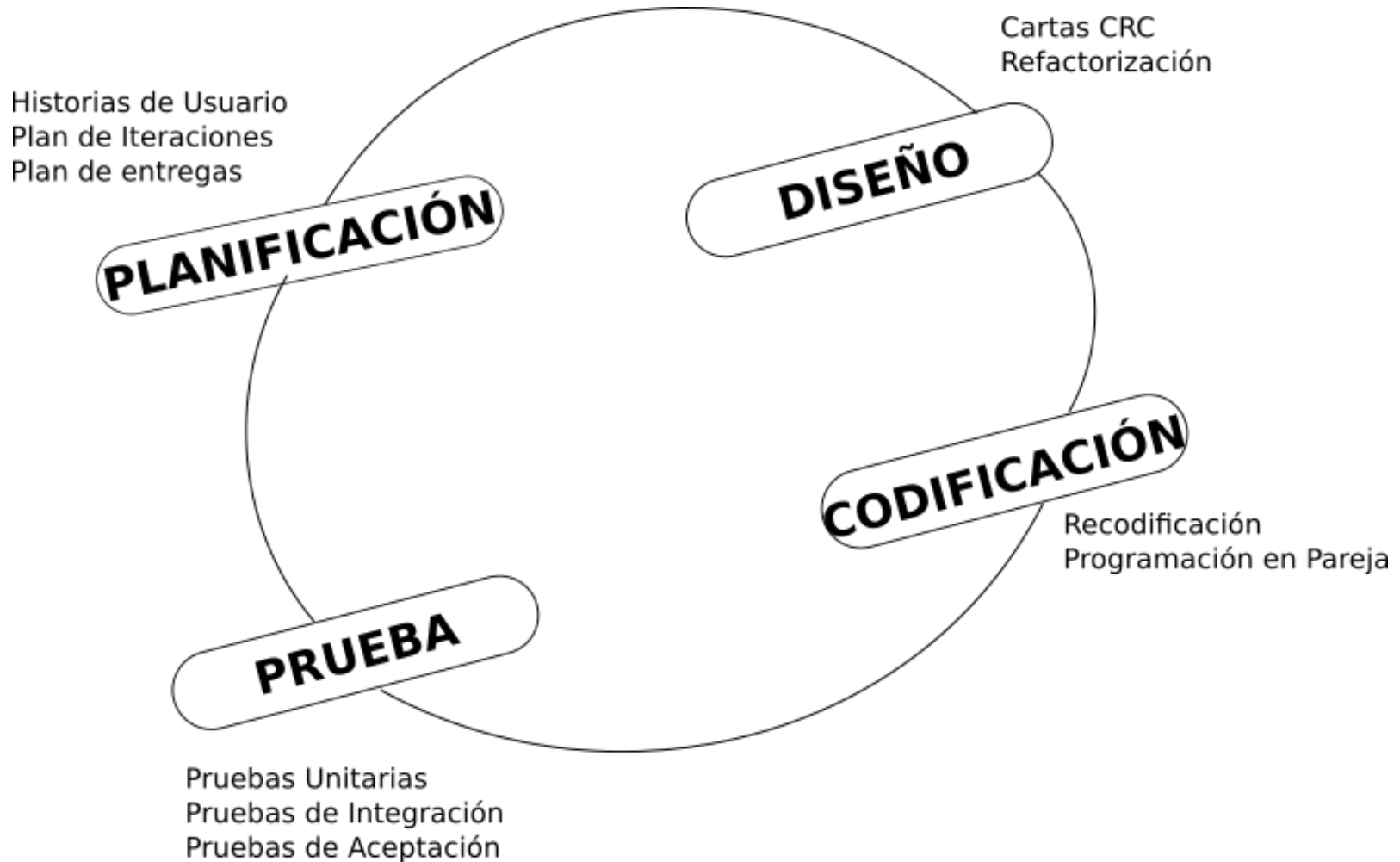
2. CERTIFICADO DIGITAL

3. REVOCACIÓN DE CERTIFICADOS

4. FIRMA DIGITAL

5. METODOLOGÍA DE DESARROLLO

METODOLOGÍA DE DESARROLLO



ÍNDICE

1. MARCO INTRODUCTORIO

2. MARCO TEÓRICO

3. MARCO APLICATIVO

1.INTRODUCCIÓN

2.PLANIFICACIÓN

3.ITERACIONES

INTRODUCCIÓN

Desarrollo de Software, adecuando fases y artefactos

Fase		Artefactos
Planificación		<ul style="list-style-type: none">• Historias de usuarios• Plan de entregas• Iteraciones
Iteración	Diseño	<ul style="list-style-type: none">• Tarjetas CRC
	Codificación	<ul style="list-style-type: none">• Cliente siempre presente
	Pruebas	<ul style="list-style-type: none">• Pruebas unitarias• Pruebas de aceptación• Pruebas de integración

ÍNDICE

1. MARCO INTRODUCTORIO

2. MARCO TEÓRICO

3. MARCO APLICATIVO

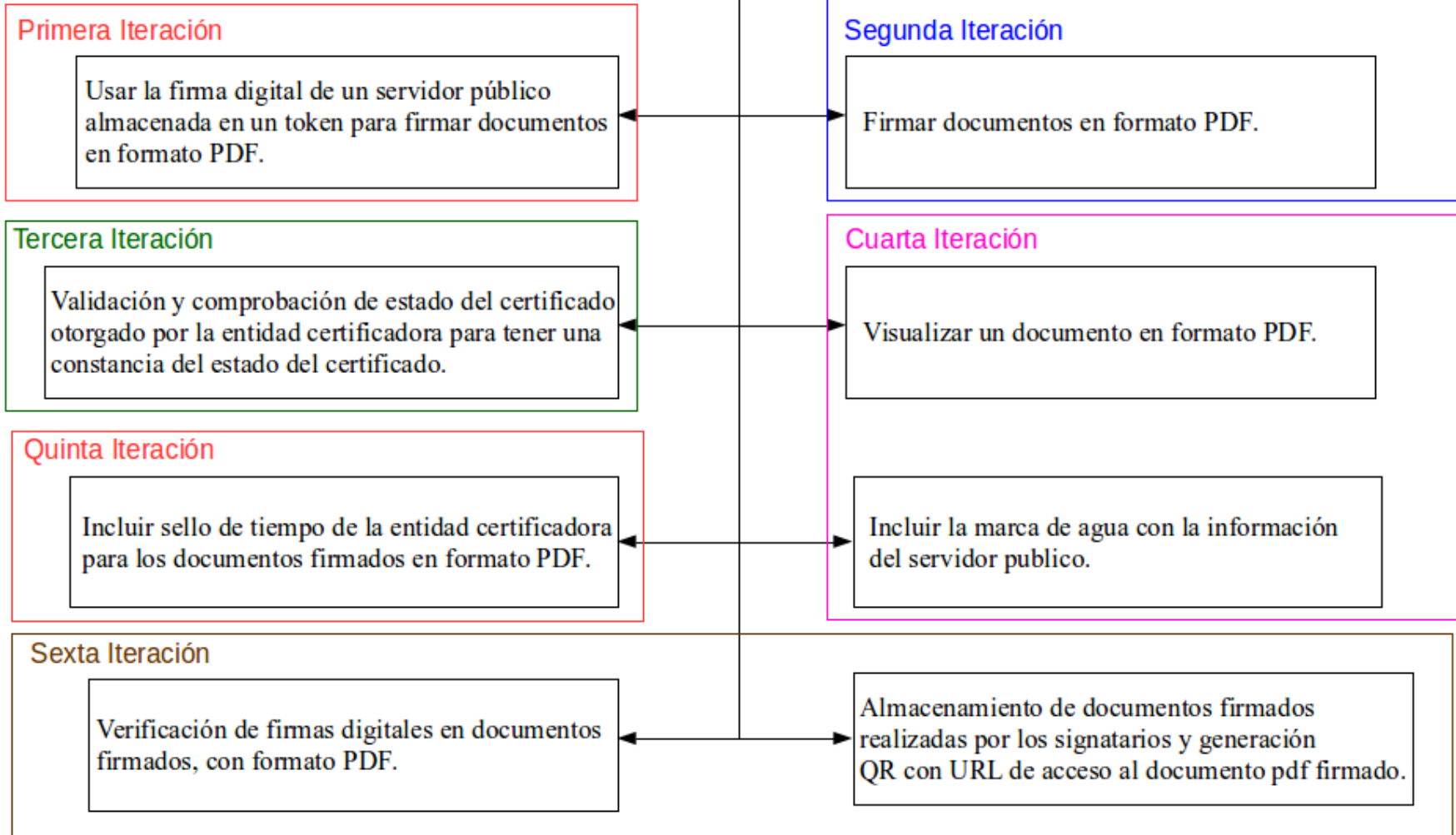
1. INTRODUCCIÓN

2. PLANIFICACIÓN

3. ITERACIONES

PLANIFICACIÓN

Historias de Usuario



ÍNDICE

1. MARCO INTRODUCTORIO

2. MARCO TEÓRICO

3. MARCO APLICATIVO

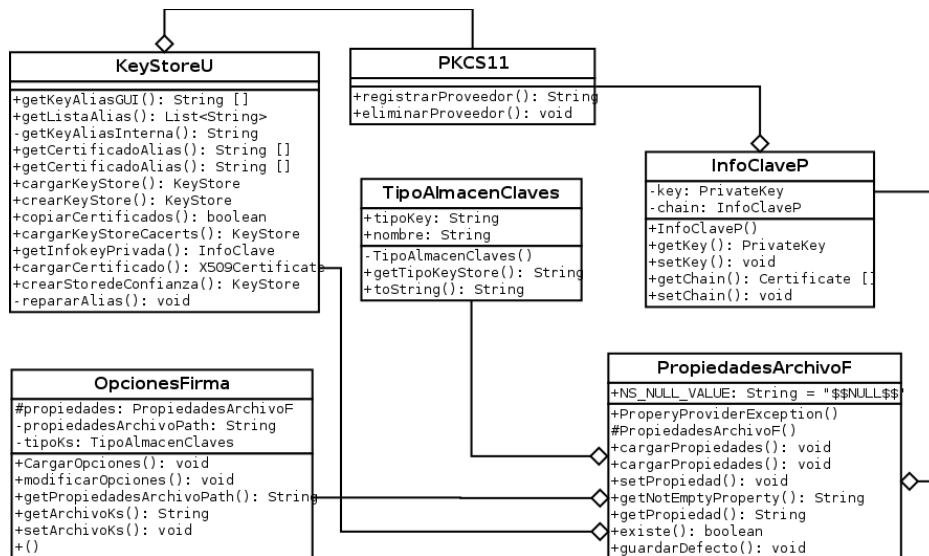
1. INTRODUCCIÓN

2. PLANIFICACIÓN

3. ITERACIONES

ITERACIONES - PRIMERA

Modelo Estructural



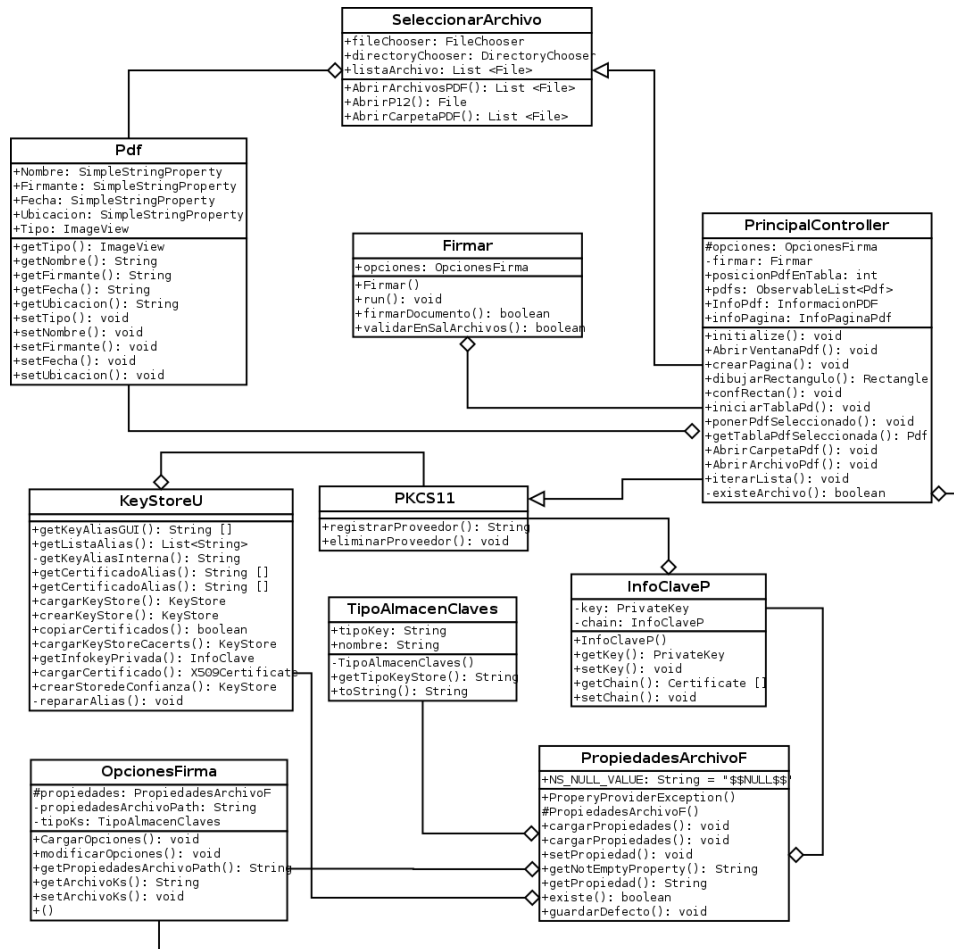
Acceso a Token o Fichero de Claves

The screenshot shows the 'Sistema Firma Digital' window. The title bar reads 'Sistema Firma Digital'. The main content area is titled 'Configuracion para elegir el tipo de KeyStore con el cual firmara.' and contains the following elements:

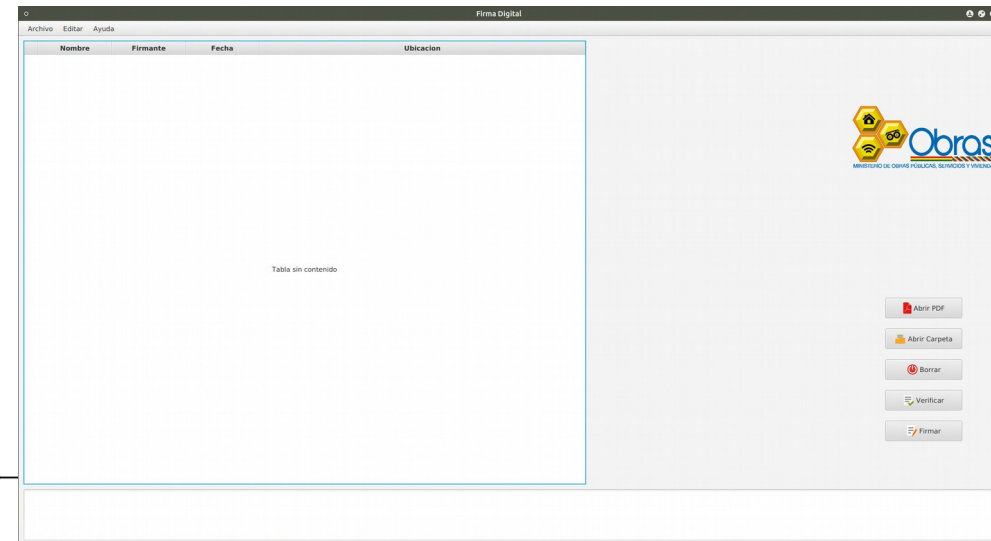
- A dropdown menu labeled 'Archivo' with a downward arrow.
- A button labeled 'Cargar Fichero'.
- A text input field containing the path '/home/armin/certificados c'.
- A label 'Contraseña' followed by a password input field with six dots.
- A checkbox labeled 'Cargar Alias del certificado' which is checked.
- A dropdown menu labeled 'cacert wot user's r...' with a downward arrow.
- A red note at the bottom: 'Nota: Es necesario escoger un tipo de firma'.
- A footer bar with four buttons: 'Ayuda ?' (with a question mark icon), 'Cancelar', 'Siguiente', and 'Finalizar'.

ITERACIONES - SEGUNDA

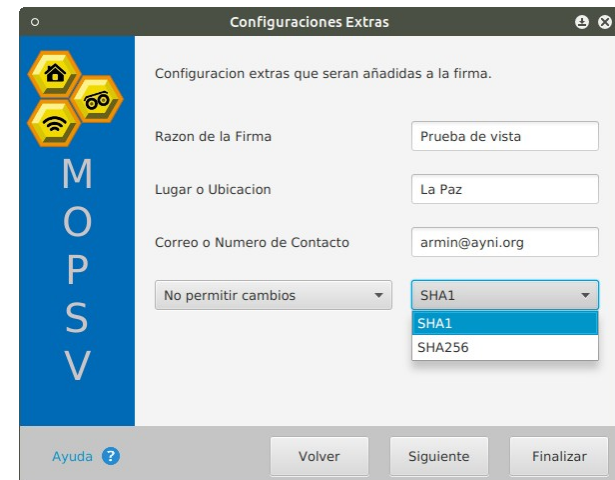
Modelo Estructural



Carga de Archivos PDF

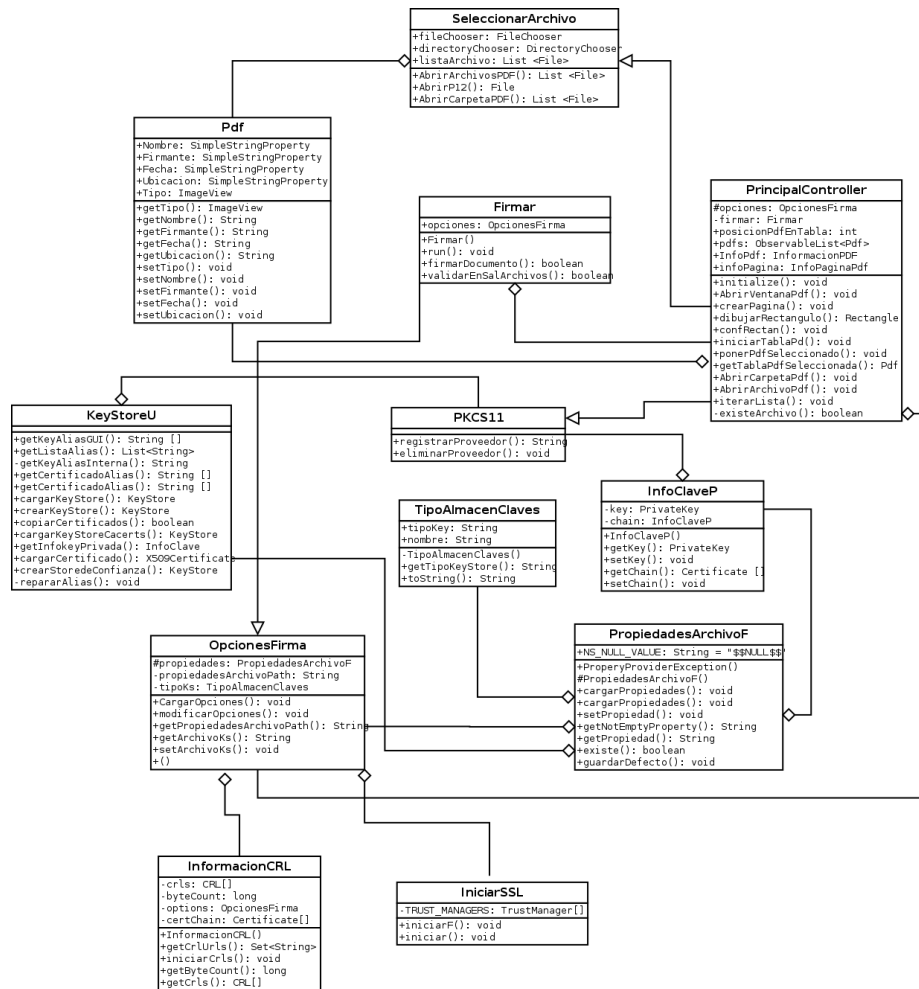


Opciones Extras para Firma Digital



ITERACIONES - TERCERA

Modelo Estructural



Consulta a OCSP y CRL

Configuración OCSP

Configuración de Servidor de consulta de Certificado y Servidor FTP respaldo de Documentos

URL de Servidor OCSP:

☒ Consultar Tambien Archivo CRL

URL Servidor FTP:

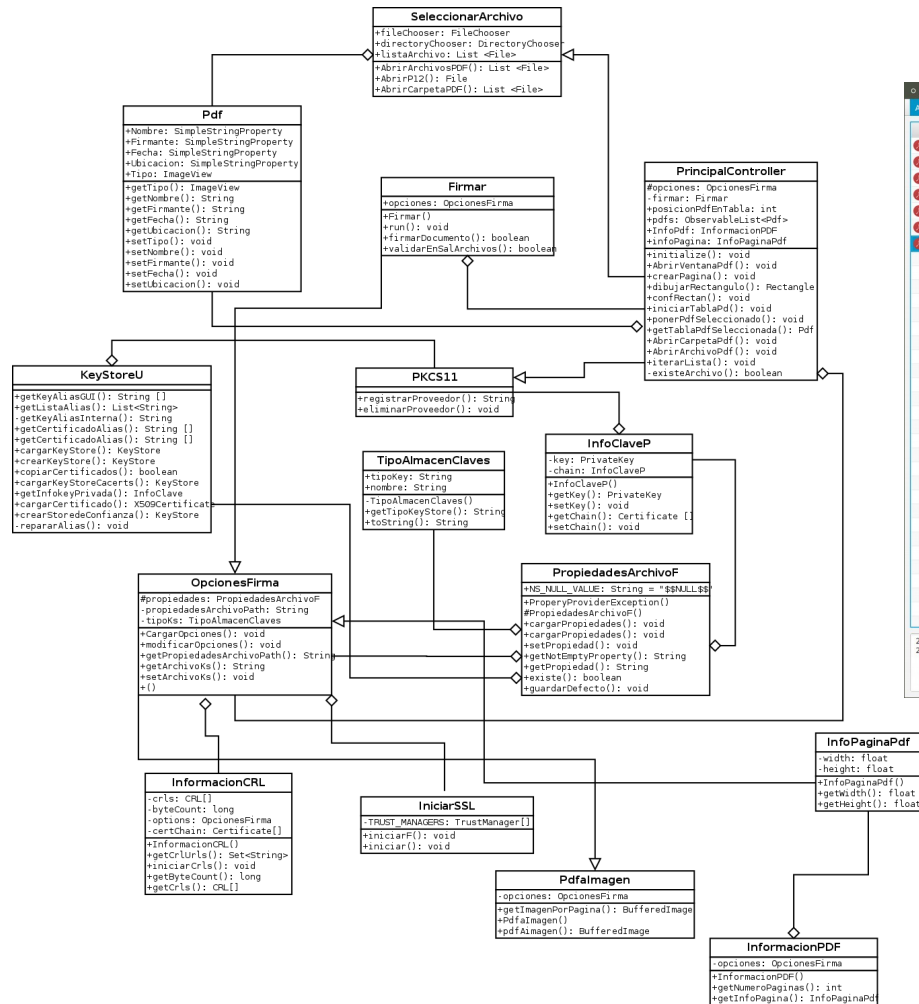
Usuario FTP:

Contraseña FTP:

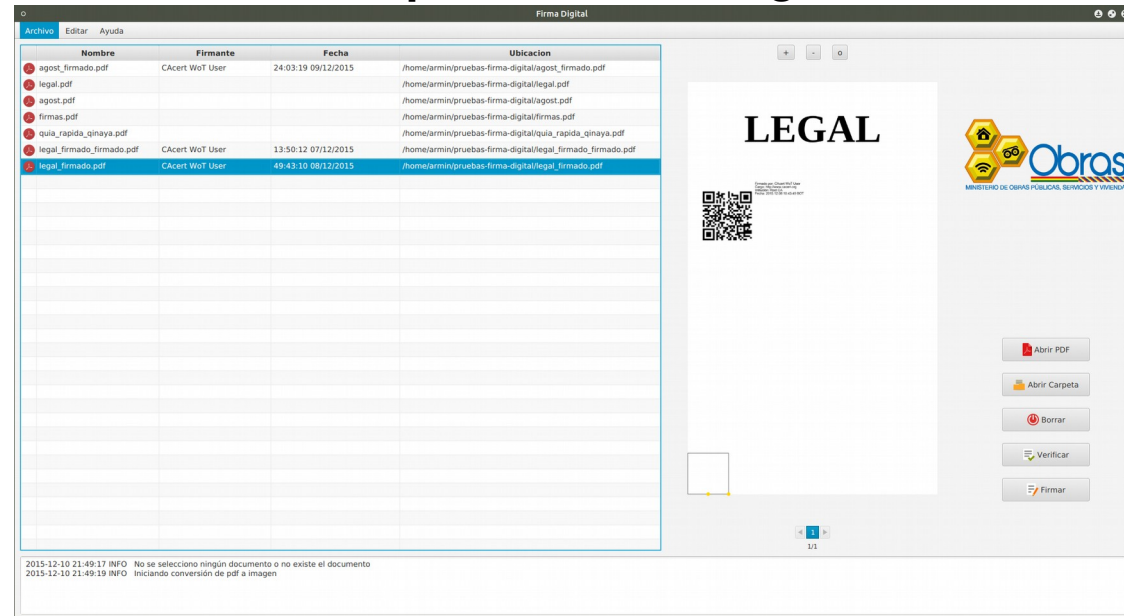
[Ayuda ?](#) [Volver](#) [Siguiente](#) [Finalizar](#)

ITERACIONES - CUARTA

Modelo Estructural

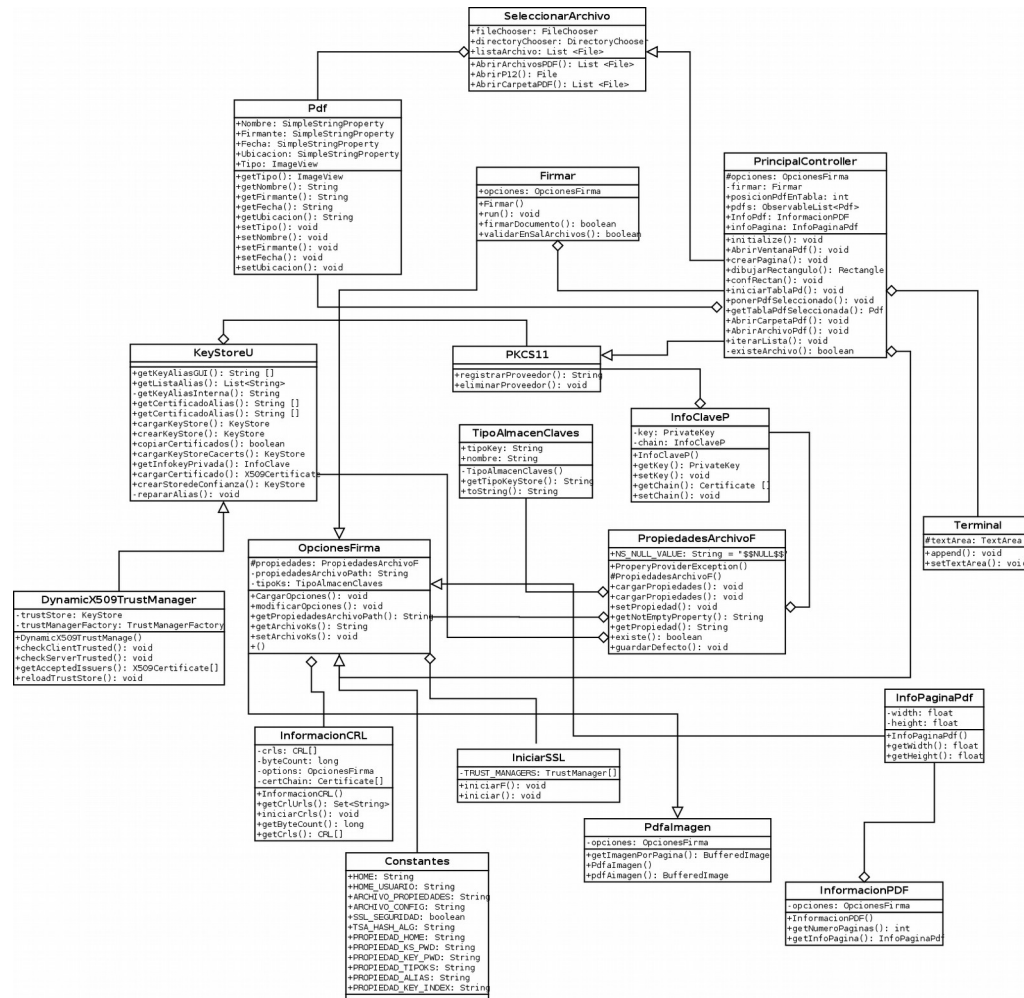


Visualización de PDF y Asignación de área para Marca de agua




ITERACIONES - QUINTA

Modelo Estructural



Consulta a servidor TSA



M
O
P
S
V

Configuración TSA

Configuración de Servidor TSA

Dirección URL de Servidor TSA

http://tsafree.net

SHA256

Usuario

Ninguno

Contraseña

Contraseña

Identificador de Firmante

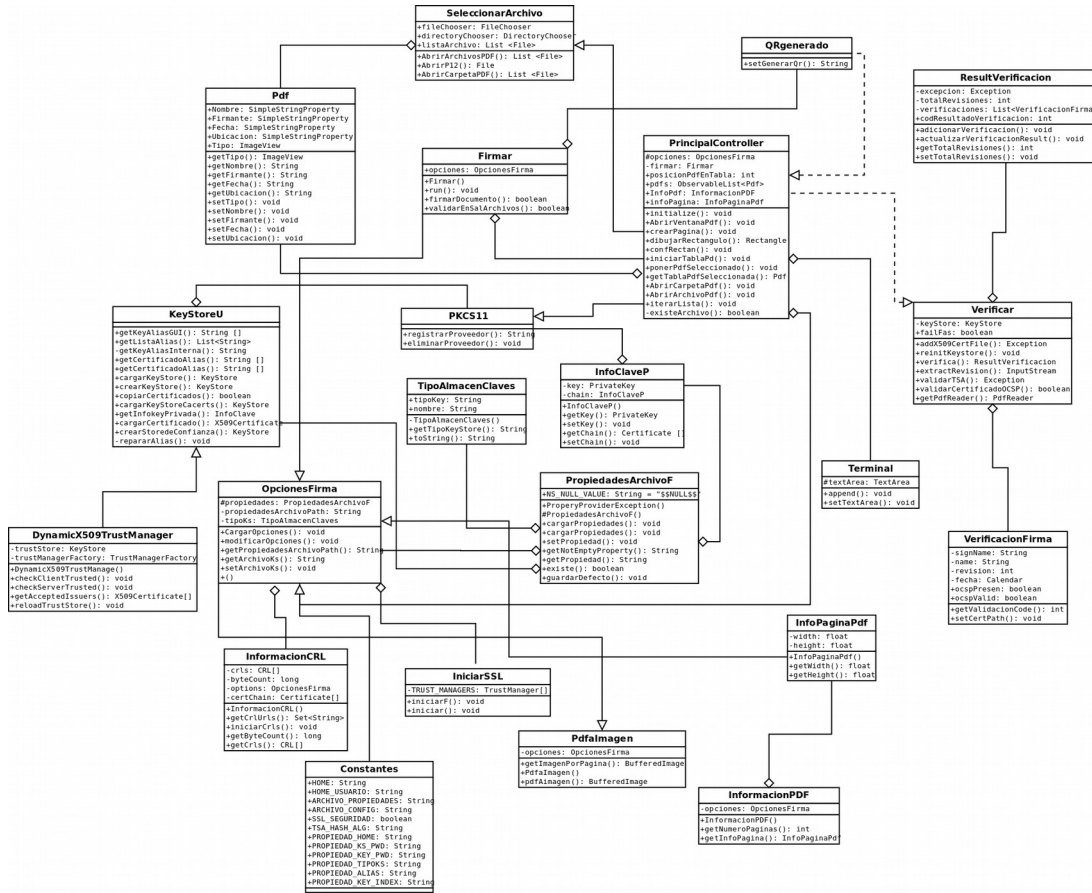
Ayuda ?

Volver

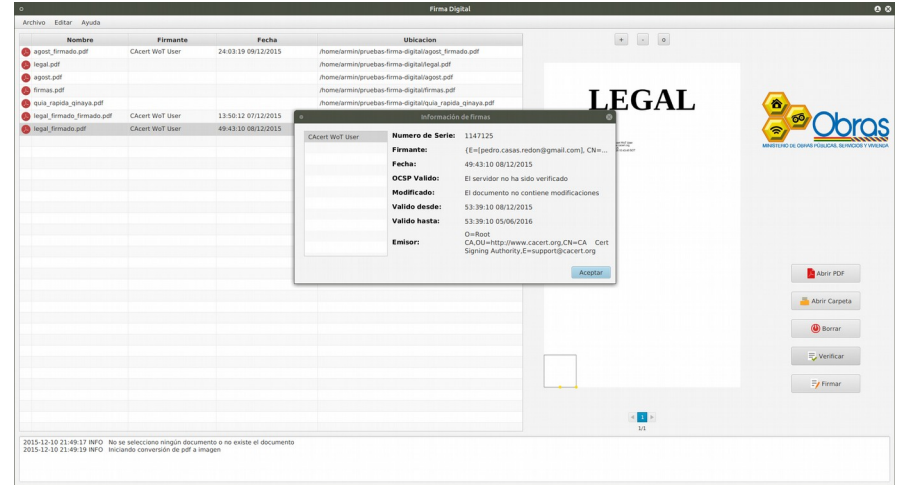
Finalizar

ITERACIONES - SEXTA

Modelo Estructural



Información de Signatarios



ÍNDICE

1. MARCO INTRODUCTORIO
2. MARCO TEÓRICO
3. MARCO APLICATIVO
4. **CALIDAD Y SEGURIDAD**
5. ANÁLISIS COSTO BENEFICIO
6. CONCLUSIONES Y RECOMENDACIONES
7. DEMOSTRACIÓN

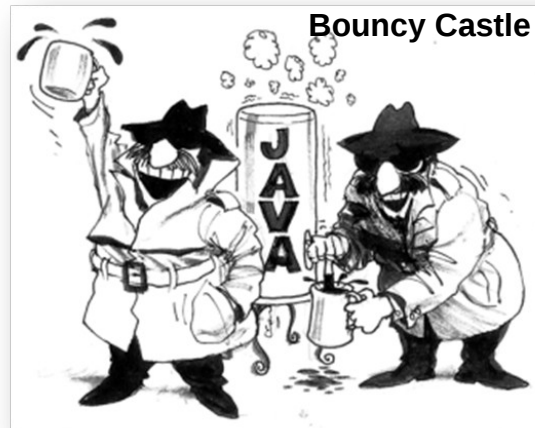
CALIDAD Y SEGURIDAD

Calidad

Escala de medición de aceptabilidad	
Funcionalidad	88.89
Mantenibilidad	91.75
Usabilidad	90.4
Portabilidad	99.79
Calidad global del sistema	92.71

Seguridad

- Seguridad a nivel de Autoridad Certificadora (CA)
- Seguridad a nivel de Usuario
- Seguridad a nivel de software



ITEXT



ÍNDICE

1. MARCO INTRODUCTORIO
2. MARCO TEÓRICO
3. MARCO APLICATIVO
4. CALIDAD Y SEGURIDAD
- 5. ANÁLISIS COSTO BENEFICIO**
6. CONCLUSIONES Y RECOMENDACIONES
7. DEMOSTRACIÓN

ANÁLISIS COSTO BENEFICIO

Costo total del Software

Detalle	Importe (\$us)
Costo de desarrollo	18000
Costo de elaboración de proyecto	800
Total	18800

Tasa Interna de Retorno

Año	Costos	Ganancias	$\frac{Ganancias - Costos}{(1-i)^n}$
1	18800	0	-18252
2	800	7600	6409
3	500	8500	7321
4	200	9300	8085
TIR			3563

Valor Actual Neto

Año	Costos	Ganancias	$\frac{Costos}{(1+i)^n}$	$\frac{Ganancias}{(1+i)^n}$	Resultado
1	18800	0	16785	0	-16785
2	800	7600	637	6058	5421
3	500	8500	355	6050	5695
4	200	9300	127	5910	5783
Σ	20300	25400	17904	18018	
VAN					114

Costo Beneficio

Por cada dólar invertido en el proyecto, la unidad tiene una ganancia de 1.25 \$us.

ÍNDICE

1. MARCO INTRODUCTORIO
2. MARCO TEÓRICO
3. MARCO APLICATIVO
4. CALIDAD Y SEGURIDAD
5. ANÁLISIS COSTO BENEFICIO
6. **CONCLUSIONES Y RECOMENDACIONES**
7. DEMOSTRACIÓN

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Se desarrollo un modelo de firma digital para documentos en formato PDF, siguiendo los lineamientos técnicos planteados por la ATT.
- Se consiguió adicionar varias firmas digitales de diferentes signatarios a un documento PDF.
- Se consiguió desplegar la información del o los signatarios, incrustada en los documentos PDF.
- Se consiguió adicionar el sello de tiempo de un servidor TSA a un documento PDF.
- Se consiguió comprobar y autenticar las firmas digitales de un documento firmado.
- Se consiguió realizar las consultas correspondientes a servidor OCSP y CRL para verificar y validar el estado de un certificado.

Recomendaciones

- Procedimientos WEB.
- Resguardo de Información.

ÍNDICE

1. MARCO INTRODUCTORIO
2. MARCO TEÓRICO
3. MARCO APLICATIVO
4. CALIDAD Y SEGURIDAD
5. ANÁLISIS COSTO BENEFICIO
6. CONCLUSIONES Y RECOMENDACIONES
7. **DEMOSTRACIÓN**

GRACIAS