Componente de Software para la Firma Digital de Documentos en formato PDF

Software Component for Digital Signature of Documents in PDF format

Alexei Zubizarreta Pérez

Universidad de las Ciencias informáticas (UCI)

azubizarreta@uci.cu

Resumen

En este trabajo se presenta una solución de firma digital de documentos en formato PDF. Se desarrolló un componente de software que dado un documento en formato PDF, permite firmar digitalmente y adjuntar la firma al documento, otorgándole integridad, autenticidad y no repudio. Una vez firmado el documento, puede ser consultado y verificado el origen así como la integridad de su contenido donde quiera que este se encuentre. Se utilizó la plataforma .NET para el desarrollo del componente, el mismo se encuentra integrado al Módulo de Gestión de Servicio Autónomo, Módulo de Registros Públicos, Módulo de Registros Mercantiles y Módulo de Digitalización de Archivos, todos pertenecientes al Sistema Automatizado para los Registros y Notarías de la República Bolivariana de Venezuela.

Palabras Claves: Certificado Digital, Firma Digital, Firma Digital de Documentos PDF.

Abstract

In this work a solution of digital signature of documents in PDF format is presented. It developed a software component that given a document in PDF format, permits to sign digitally and include the signature to the document, offering it integrity, authenticity and not repudiation. Once signed the document, it can be consulted and verified the origin as well as the integrity of its content wherever be found. The .NET platform was utilized for the development of the component, the same one is found integrated to the Gestión de Servicio Autónomo Module, Registros Públicos Module, Registros Mercantiles Module and Digitalización de Archivos Module, all belonging to the Automated System for the Registries and Notaries of the Republic Bolivariana of Venezuela.

Keywords: Digital Certificate, Digital Signature, Documents Digital Signature.

Introducción

El creciente intercambio a través de internet y el uso de las Nuevas Tecnologías de la Información y las Comunicaciones, han permitido que el documento electrónico cada vez gane más terreno en las plataformas digitales como medio de intercambio de información, así como en los sectores gubernamentales y en específico en el ámbito jurídico. La seguridad de los documentos electrónicos es hoy en día una necesidad ya que han existido muchos casos de falsificación de información.

En aras de dotar al documento electrónico de la seguridad que posee el documento en papel con la firma manuscrita, se han creado herramientas que permiten validar la veracidad del contenido. Una de ellas es la firma hológrafa, la cual es obtenida a través de escaneo de firmas manuscritas y almacenadas en formato digital, otra es la **Firma Digital** la cual es objeto de implementación en el presente artículo como medio de seguridad de los documentos electrónicos, está última le otorga las propiedades de

autenticidad (identidad del firmante), integridad (no alteración del contenido) y no repudio (no repudio de haber firmado el documento).

En el proyecto de Registros y Notarías de la República Bolivariana de Venezuela, se identificaron tres procesos documentales donde la seguridad de los documentos es de vital importancia.

- Gestión de Servicio Autónomo: **Actos de Última Voluntad, Legalizaciones y Negativas Registrales.**
- Registro Público y Registro Mercantil: **Inscripción de Documentos.**
- Digitalización de Archivos: **Exportación de Unidades Documentales al Servicio Autónomo de Registros y Notarías (SAREN).**

En estos procesos documentales se introdujo la firma digital de los documentos electrónicos en formato PDF utilizando un componente de software integrado a la solución de automatización.

Metodología

Para el desarrollo de la solución se ha seguido la metodología siguiente:

-Revisión teórica.

-Elección de las herramientas de desarrollo.

-Diseño e implementación del componente de software de firma digital.

Revisión teórica

La firma digital de un documento es un conjunto de datos que son el resultado de aplicarle una secuencia de algoritmos matemáticos, los cuales le confieren garantías de seguridad.

Para la comprensión de los algoritmos que se presentan en la solución se detallan algunas definiciones con el objetivo de tener una visión más clara de los procesos de firmas digitales.

Hash (Digesto): Es un algoritmo que dado un bloque de datos de cualquier longitud, produce uno de longitud fija. El resultado es más pequeño que el original. Si se cambia un bit del dato original, el resultado será diferente.

SHA1: Es un algoritmo resumen (Secure Hash Algorithm) que toma un mensaje de cualquier longitud menor que 2^{64} bits y produce un digesto de 160 bits.

RSA: Es un algoritmo propuesto por Ron Rivest, Adi Shamir y Leonard Adleman en 1978. Se usa para encriptar y desencriptar datos, para firma digital y verificación (y, por lo tanto, para la integridad de los datos).

El diseño de la solución está basado en los procesos de firma digital y verificación, los cuales se describen a continuación:

Proceso de firma digital de un documento en formato PDF

a) Se calcula un resumen o digesto del documento mediante una función hash (SHA1).

b) Se encripta el resumen con la clave privada del firmante mediante la función RSA obteniéndose la firma digital.

c) Se adjunta la firma digital al documento PDF.

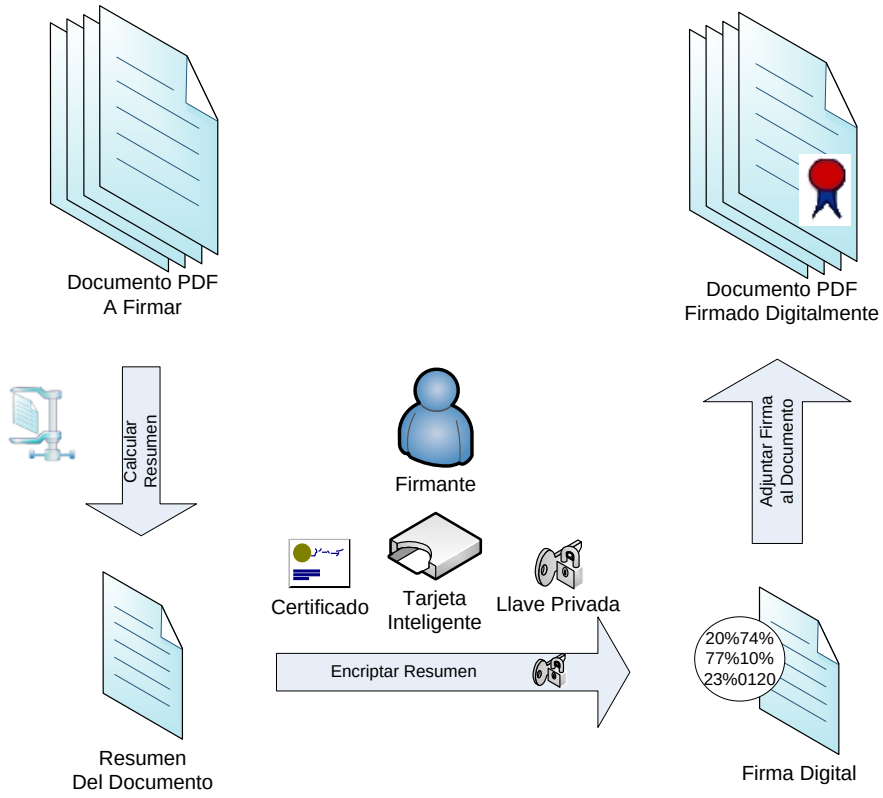

Figura 1. Representación del proceso de firma digital en un documento en formato PDF.

Proceso de verificación de firma digital en un documento en formato PDF

a) Se separa la firma digital del documento.

b) Se calcula un resumen (resumen1) del documento mediante la función SHA1.

c) Se desencripta la firma digital con la llave pública del firmante mediante la función RSA, obteniéndose el resumen (resumen0) original del documento.

d) Se compara el resumen1 con el resumen0. En caso de ser iguales, la firma digital del documento es válida. En caso contrario la firma digital no se corresponde con el documento por lo tanto no es válida.

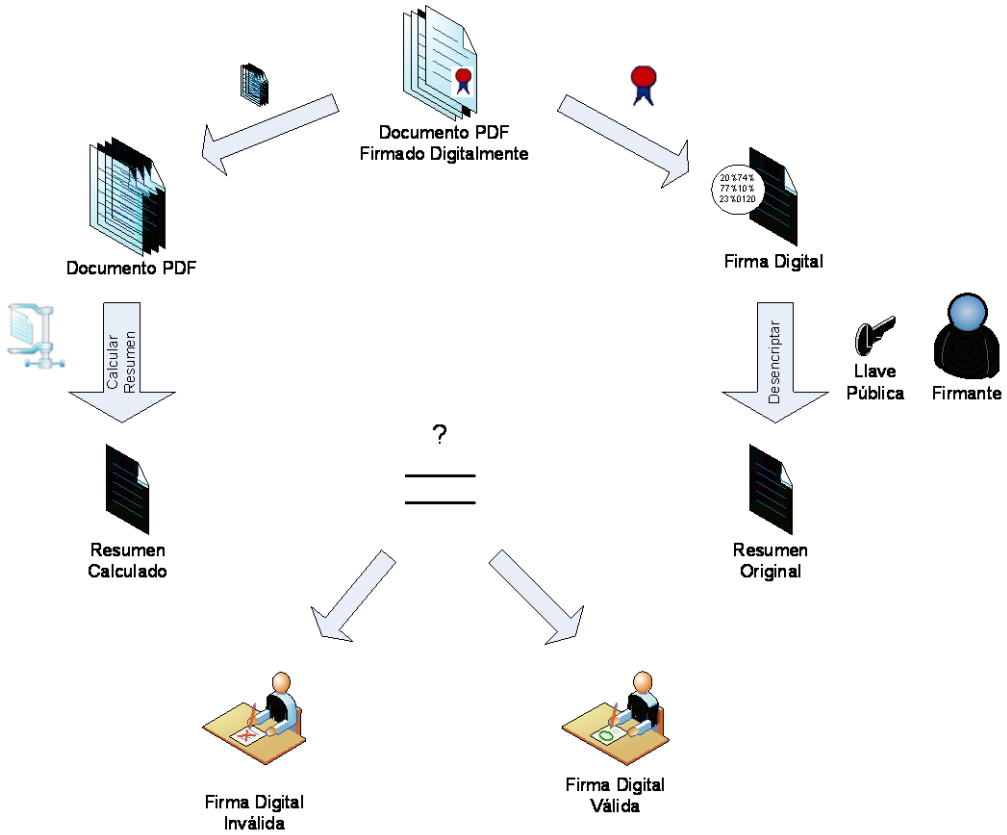

Figura 2. Representación del proceso de verificación de firma digital en un documento en formato PDF.

Elección de las herramientas de desarrollo

Para el desarrollo del componente, se utilizó la plataforma .NET y la herramienta Visual Studio de Microsoft. Esto permitió acortar los tiempos de desarrollo gracias a las librerías de clases de seguridad ya implementadas.

Diseño e implementación del componente de software de firma digital

Para la implementación de la solución se utilizaron las librerías iTextSharp [1]y CAPICOM[2].

A continuación se presenta el diseño de clases utilizado en el componente FirmaDocPDF.

---

[1] Librería desarrollada por Bruno Lowagie y Paulo Soares, se especializa en el manejo de documentos PDF. Sitio Web http://itextsharp.sourceforge.net

[2] Librería desarrolla por Microsoft, se especializa en los temas criptográficos y en el manejo de dispositivos Smart Cards. Se encuentra disponible en la dirección siguiente: http://www.microsoft.com/downloads/details.aspx?FamilyID=860EE43A-A843-462F-ABB5-FF88EA5896F6&displaylang=es

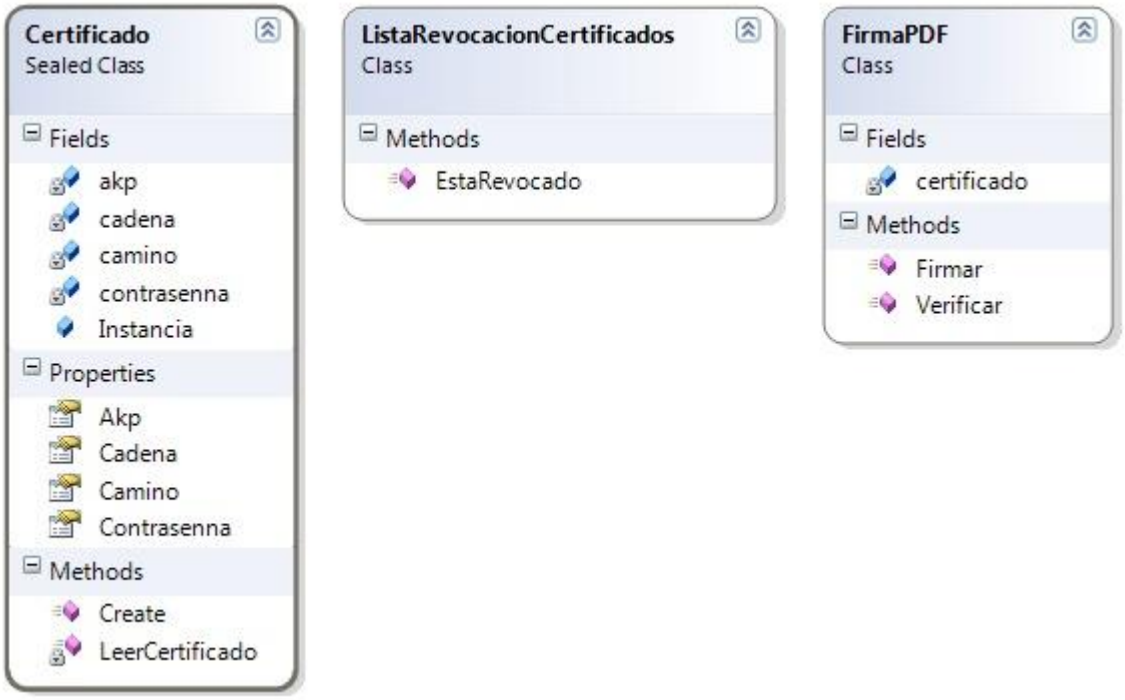

Figura 3. Diagrama de clases del componente *FirmaDocPDF*.

A continuación se muestra un ejemplo de utilización del componente *FirmaDocPDF* haciendo uso de un certificado en formato Pfx[3], para la firma de un documento PDF, el fichero de salida es un documento firmado digitalmente con la firma digital incrustada en el documento.

```
string CaminoCertificado = @"C:\\certificado.pfx";

string Contrasenna = "contraseña";

string CaminoPDFEntrada = @"C:\\1.pdf";

string CaminoPDFSalida = @"C:\\1_firmado.pdf";

string CaminoCertificado = @"C:\\certificado.pfx";

string CaminoCRL = @"C:\\cacrl.pem";

string Razon = "DIGITALIZACION";

string Contacto = "correo@mij.gov.ve";

string Lugar = "CENTRO DE DIGITALIZACION REGISTROS Y NOTARIAS";

 if (!ListaRevocacionCertificados.EstaRevocado(CaminoCertificado, Contrasenna, CaminoCRL))

{

    FirmaPDF.Firmar(CaminoPDFEntrada, CaminoPDFSalida, CaminoCertificado, Contrasenna, Razon,

                        Contacto, Lugar);

}

else
```

[3] Pfx es un fichero en formato binario basado en el estándar PKCS#12 el cual contiene un certificado y la llave privada.

```
{
    //Añadir Código. Certificado Revocado
}
```

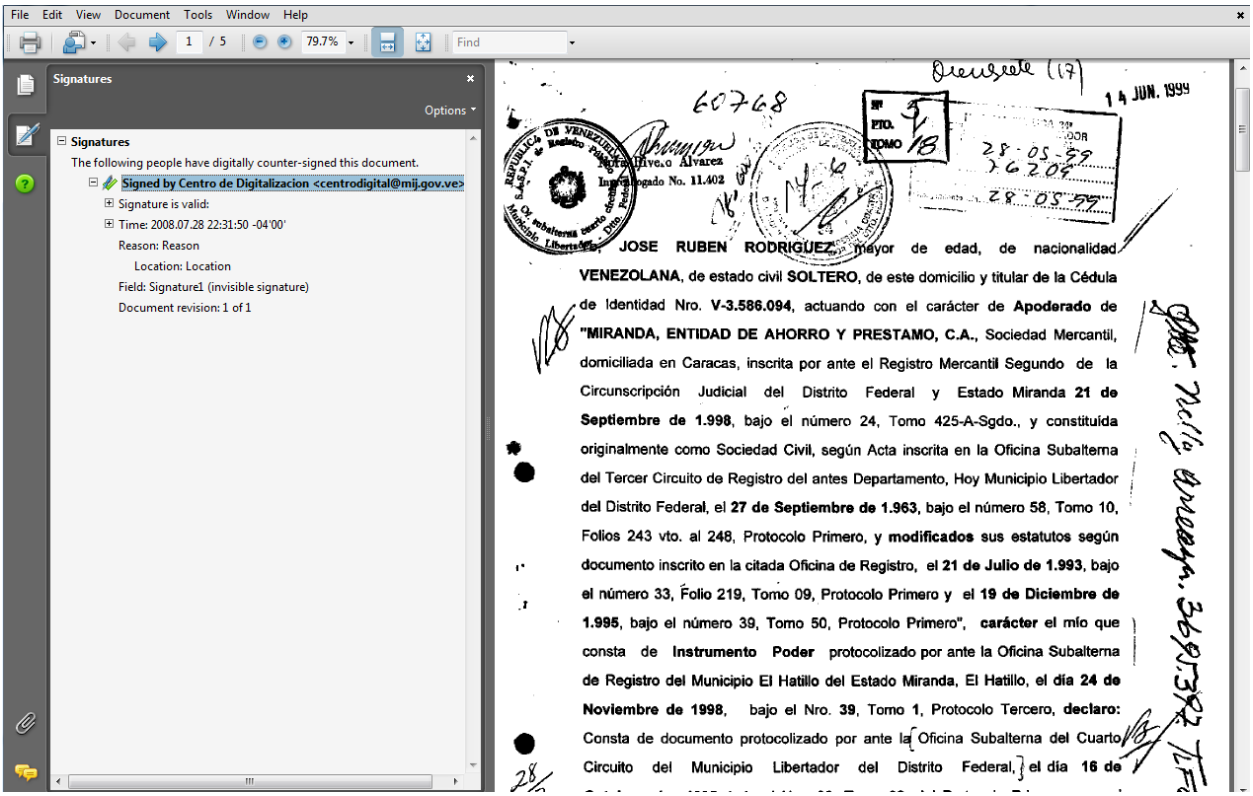

Figura 4. Documento Firmado Digitalmente en el Centro de Digitalización del Servicio Autónomo de Registros y Notarías (SAREN) de la República Bolivariana de Venezuela.

Conclusiones

El desarrollo del componente de software para la firma digital de documentos en formato PDF, ha permitido otorgarle seguridad jurídica a los documentos en los procesos de Inscripción de documentos, Digitalización de Archivos, Actos de Última Voluntad, Legalizaciones, y Negativas Registrales, pertenecientes al Sistema Automatizado de Registros y Notarías. Además este componente puede ser usado para firmar documentos en formato PDF en cualquier proceso documental automatizado, confiriéndole autenticidad, integridad y no repudio a dichos documentos.

Referencias Bibliográficas

[1] Andrew Nash, William Duane, Celia Joseph, Derek Brink. (2001) PKI: Implementing and Managing E-Security.

[2] Bruno Lowagie (2007) iText in Action Creating and Manipulating PDF.

[3] Carlisle Adams, Steve Lloyd (2002) Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition.

[4] Tom St Denis, Simon Johnson. (2007) Cryptography for Developers.

[5] Kapil Raina. (2003) PKI Security Solutions for the Enterprise: Solving HIPPAA, E-Paper Act, and Other Compliance Issues.

[6] Steve Burnet, Stephen Paine. (2001) RSA Security's Official Guide to Cryptography.