Universidad Latinoamericana de Ciencia y Tecnología

Facultad de Ingeniería
Escuela de Ingeniería Informática

Trabajo final para optar por el grado de Licenciatura en Ingeniería Informática con énfasis en Gestión de Recursos Tecnológicos

Tema: Firma Digital

Estudiante: Orlando Valverde Venegas
Cédula: 5-0292-0294

Profesor: Miguel Pérez Montero

III Cuatrimestre 2007

Índice

Firma Digital: Reseña e Implementación Práctica

Orlando Valverde Venegas [1]

Resumen: El término firma digital en el ámbito informático es bastante común y muy amplio en conceptos teóricos, no obstante, el cómo implementarla en una aplicación tiene otra connotación; es por ello que en este artículo se aborda el tema desde una perspectiva práctica mediante la explicación de un componente DLL desarrollado en Microsoft Visual Basic que muestra los pasos a seguir para generar un archivo firmado digitalmente a partir de un archivo origen almacenado en disco; también se muestra la forma de verificar el archivo firmado así como la obtención del texto en claro a partir de éste, por último, veremos como enviar un mensaje de correo electrónico firmado digitalmente. De modo, que al completar la lectura del artículo se habrá obtenido un criterio más amplio e integral tanto a nivel técnico como conceptual de como incorporar el firmado digital en una aplicación.
Palabras claves: capicom, firma digital, certificado digital, criptografía, hash.

Abstract: The term “digital signature” in the computer field is quite common and very wide in theoretical concepts. Nevertheless, implementing it in an application has another connotation. For that reason, this article approaches the subject from a practical perspective by means of the explanation of a component DLL developed in Microsoft Visual Basic. This component shows the steps followed to generate a file signed digitally from a file stored originally in a disc. How to verify the signed file is also showed, as well as how to obtain the text in clear from the original one. Finally, we will see the process to send a digitally signed e-mail. As a result, this research will allow the reader to have a wider and more integral criterion in a level both technical and conceptual of how to incorporate the digital signed in an application.
Keywords: capicom, digital signature, digital certificate, cryptography, hash.

---

[1] Bachiller en Ingeniería de Sistemas Informáticos. Candidato al título de Licenciatura en Ingeniería Informática con énfasis en Gestión de Recursos Tecnológicos. Ulacit. Correo electrónico: orlvalve13@yahoo.es

I. Introducción

Vivimos en un mundo cada vez más globalizado y competitivo, en donde los esquemas tradicionales de casi todo lo que conocemos están evolucionando rápidamente hacia formas innovadoras y cada vez más estrechamente relacionadas con la tecnología. Las TIC's (tecnologías de la información y la comunicación) crecen a pasos agigantados, provocando un efecto directo en la forma en que interactuamos como sociedad; hoy en día, esta interacción a través de medios electrónicos y digitales juega un papel verdaderamente crucial a nivel mundial. Temas como comercio electrónico y economía digital son cada vez más comunes e inherentes a nuestra forma de vida.

El panorama anterior repercute directamente en la forma en que nos comunicamos, ya que permite la generación de transacciones no presenciales a través de redes públicas como es el caso de Internet, en donde resulta imposible controlar que lo transmitido no sea interceptado; es por ello, que la transferencia de datos e información debe ser íntegramente garantizada, para que su uso resulte seguro. Es en este escenario, en donde hace su incursión la firma digital, misma que garantiza aspectos como la autenticidad, la integridad y el no repudio en un documento electrónico, características que vienen de la mano con lo que se conoce como la criptografía de llave pública.

Este artículo no solamente intenta reseñar conceptos teóricos en relación con la firma digital, sino que pretende ir un paso más allá, clarificando su uso e implementación mediante un enfoque meramente práctico; se mostrará mediante un código fuente funcional, cómo firmar un archivo de texto y cómo verificar su firma; además se ejemplificará el uso de certificados digitales para firmar mensajería de correo electrónico. Para tal cometido, previamente me he dado a la tarea de investigar, desarrollar y probar una pequeña aplicación de firmado digital, este aplicativo lo desarrollé, haciendo uso de la herramienta de programación Microsoft Visual Basic 6.0 y consiste de un proyecto EXE estándar que invoca a un DLL ActiveX, en donde encapsulé los métodos de firma; dicho DLL hace uso de

CAPICOM que es un componente de Microsoft, desde el cual se puede acceder a funciones criptográficas avanzadas; además, para el envío de correo electrónico hago uso de CDO (Collaboration Data Objects) y ADO (ActiveX Data Objects).

Al llegar a este punto es natural que surjan varias interrogantes, ¿Qué es firma digital? ¿Cómo funciona? ¿Qué es criptografía de llave pública? ¿Cómo implemento firma digital en una aplicación? ¿Valor legal?, pues bien, antes de explorar en detalle el aplicativo de ejemplo conviene explicar y dejar claros estos y otros conceptos que están muy ligados con el mundo de la firma digital.

II. Validez Legal

En Costa Rica la ley No. 8454 del 30 de agosto del 2005 faculta la utilización de la firma digital, al respecto el artículo 9 indica:
Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera, tanto la digital como la manuscrita (Ley 8454, 2005).

III. Conceptos Relacionados con la Firma Digital

Criptografía

El propósito básico de la criptografía es ocultar la información a quien no esté autorizado para verla; se divide en dos grandes ramas: la criptografía de llave privada o simétrica y la criptografía de llave pública o asimétrica.

Criptografía Simétrica

La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes, siempre y cuando anteriormente se hayan intercambiado la clave correspondiente. La simetría se refiere a que las partes tienen la misma llave, tanto para cifrar como para descifrar (Universidad de Murcia, 2007).

Criptografía Asimétrica

La criptografía empezó realmente a ser popular cuando Whitfield Diffie y Martin Hellman de la Universidad de Standford hicieron público en 1976 (New Directions in Cryptography) un algoritmo de encriptación de clave pública. Hasta el momento, los métodos eran simétricos, permitían almacenar de forma segura la información, pero tenían el inconveniente de que para transmitir la información había que intercambiar la contraseña, mientras que, con el sistema de clave pública, las claves son diferentes pero complementarias (Llorente, I.M, 2006).

La criptografía asimétrica, es aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada (Universidad de Murcia, 2007). Es importante hacer notar que lo codificado con una clave privada, requiere su correspondiente clave pública para ser descodificado y lo codificado con una clave pública, sólo puede ser descodificado con su clave privada, es precisamente éste el método empleado por la firma digital.

Hasta la fecha han aparecido muchos algoritmos asimétricos, la mayoría de los cuales son inseguros; otros son poco prácticos, bien sea porque el criptograma es considerablemente mayor que el mensaje original o bien, porque la longitud de la clave es enorme. El más popular por su sencillez es RSA, que ha sobrevivido a multitud de ataques, si bien necesita una longitud de clave considerable; se recomiendan claves al menos de 1024 bits. (Lucena, L.M, 2003).

Algoritmo RSA

Este sistema de clave pública fue diseñado en 1977 por los profesores del MIT (Massachusetts Institute of Technology) Ronald R. Rivest, Adi Shamir y Leonard M. Adleman, de ahí las siglas con las cuales es conocido. La seguridad de RSA radica en la dificultad de la factorización de números grandes: es fácil saber si un número es primo, pero es extremadamente difícil obtener la factorización en números primos de un entero elevado, debido no tanto a la dificultad de los

algoritmos existentes, sino al consumo de recursos físicos (memoria, necesidades hardware, incluso tiempo de ejecución) de tales algoritmos (Villalón, H.A, 2006).

Este algoritmo fue registrado el 20 de setiembre de 1983 y el 20 de setiembre del 2000, tras 17 años, expiró la patente de los Laboratorios RSA, con lo cual, pasó a ser un algoritmo de dominio público (Cea, A.J, 2000).

Función Hash

Es una función matemática que toma un texto grande y genera una secuencia de longitud fija. La bondad de una función hash se mide por la distribución (aleatoriedad) de los resultados. Ejemplos de algoritmos hash son MD5 y SHA (Universidad de Murcia, 1999).

SHA (Secure Hash Algorithm)

La familia SHA (Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST). El primer miembro de la familia fue publicado en 1993, es oficialmente llamado SHA. Sin embargo, hoy día y de forma no oficial se le llama SHA-0 para evitar confusiones con sus sucesores. Dos años más tarde, el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces, cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 -llamándose SHA-2 a todos ellos- (Wikipedia, 2007).

PKI (Infraestructura de Clave Pública)

Se refiere a una estructura de hardware, software, personas, procesos y políticas que emplean tecnología de firma digital, para proveer una asociación verificable entre una llave pública y un suscriptor específico que posee la llave privada correspondiente (La Gaceta, 2006). El acrónimo PKI deriva de "Public Key Infrastructure" y es la forma común de referirse a un sistema complejo necesario

para la gestión de certificados digitales y aplicaciones de Firma Digital. Una PKI construida adecuadamente brinda autenticidad, confidencialidad, integridad y no repudio.

Certificados Digitales

La función básica de un certificado digital es establecer un vínculo entre la clave pública de un usuario y su identidad, para ello contiene información como la identidad del usuario, su clave pública, período de validez, ente emisor (autoridad certificadora), firma del emisor y otras.

Firma Digital

Conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permite verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico (Ley 8454, 2005). Por ende, al firmar digitalmente un documento, se crea una "huella digital" de éste, la cual es única y puede ser creada solamente por el firmante del mismo. Entonces, es claro que la firma digital depende del documento que la origina y que al combinar el documento, su firma digital y el certificado digital, se puede verificar la autenticidad y la integridad del documento, así como la identidad del autor de la firma.

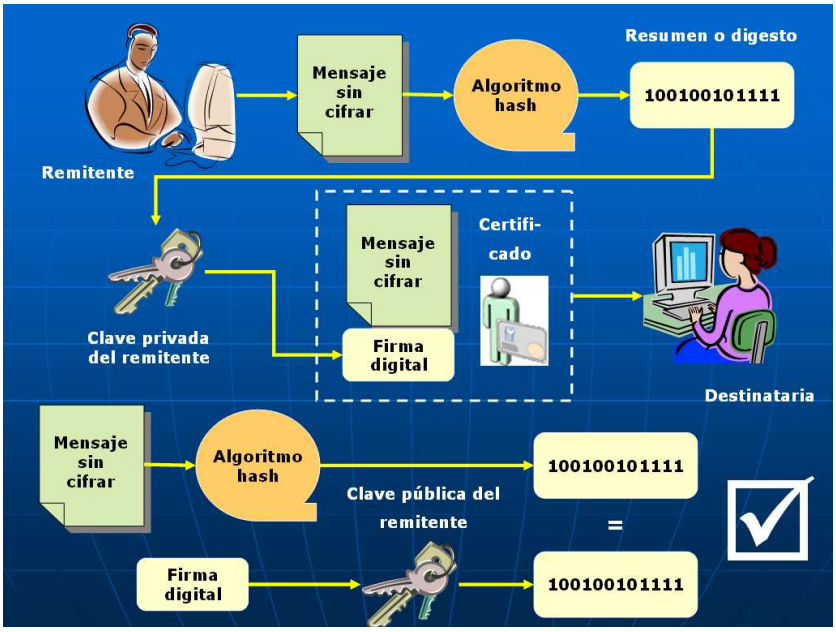
Proceso de Autentificación

Dos puntos I y II mantienen comunicación, conociendo I la llave pública de II. Desde el punto II, se envía un documento firmado digitalmente y un criptograma asociado que sólo es posible hacerse, utilizando su clave privada. Entonces I, utilizando la llave pública de II genera un criptograma reflejo, compara ambos criptogramas y, si son iguales, el documento es auténtico. Si alguna parte del documento o parte de la firma se modifica, aunque sea ligeramente, entonces el procedimiento de autentificación indicará que el documento no es auténtico. Si una llave pública autentifica un documento firmado, entonces el documento fue firmado con la correspondiente llave privada, es decir, si un individuo tiene asociada la llave pública que autentifica el documento, entonces, éste fue efectivamente

firmado por ese individuo. A diferencia de la firma autógrafa, que es biométrica y efectivamente prueba el acto personal de firma, la firma digital sólo prueba que se utilizó la llave privada del sujeto y no necesariamente el acto personal de firma. En consecuencia, no es posible establecer con total seguridad que el individuo firmó un documento, sino que sólo es posible demostrar que el individuo es el responsable de que el documento se firmara con su llave privada. En otras palabras, si un documento firmado corresponde con la llave pública de un sujeto, entonces el sujeto, aunque no lo haya hecho, debe reconocer el documento como auténtico (Marrero, T.Y, 2006).

En la figura 1 se brinda una descripción gráfica que sirve como complemento a lo ya expuesto del proceso de Autentificación.

Figura 1: Protocolo de Firma Digital



Fuente: (Hess, A.C, 2007)

En síntesis, el protocolo de firma digital se puede resumir de la siguiente forma:

1. El emisor genera un hash o digesto o resumen del documento por firmar.
2. El emisor cifra el resumen con su clave privada, ésta es la firma del documento.
3. El emisor envía el documento junto con el resumen cifrado al receptor.

4. El receptor al recibir el mensaje genera un nuevo resumen del documento recibido, usando la misma función que el emisor.
5. El receptor descifra el resumen recibido, usando la clave pública del emisor.
6. Si el resumen o hash obtenido de la firma del documento coincide con el resumen que el receptor ha generado, la firma es válida.

Almacenes de certificados

Los certificados digitales se almacenan en ubicaciones seguras denominadas almacenes de certificados. Un almacén de certificados puede contener además de certificados, listas de revocación de certificados (CRL) y listas de certificados de confianza (CTL). Cada usuario tiene un almacén personal denominado "MY store" que es donde se almacenan los certificados del usuario (Microsoft, 2006).

CAPICOM (Cryptographic API Component Object Model)

Es un componente de Windows que proporciona servicios a los programas que habilitan la seguridad basada en cifrado. Esto incluye la funcionalidad para la autenticación que utiliza firmas digitales, para envolver mensajes, para cifrar y descifrar datos (Microsoft, 2007).

S/MIME (Secure / Multipurpose Internet Mail Extensions)

Es un protocolo que añade firmas digitales y encriptación a los mensajes MIME. MIME es el formato estándar propuesto para correo electrónico que define cómo se estructura el cuerpo de un mensaje, permite incluir texto enriquecido: gráficos, audio, etc. Sin embargo, MIME por sí mismo no proporciona ningún servicio de seguridad; el propósito de S/MIME es proporcionar estos servicios de seguridad, siguiendo la sintaxis definida en PKCS#7 (CA Banesto, 2007).

PKCS #7 (Cryptographic Message Syntax Standard)

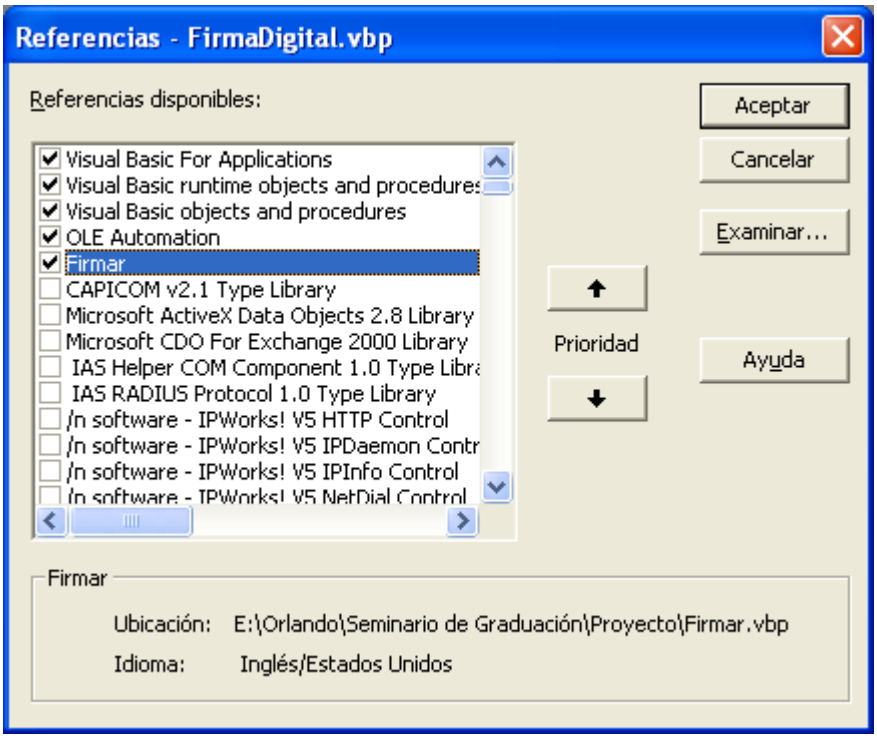
Este estándar es un conjunto de normas para firmar y encriptar documentos, normalmente usado en el correo electrónico para lograr autenticidad y privacidad de los datos e información contenida (CA Banesto, 2007).

IV. Implementación Práctica

Para analizar más de cerca la integración y funcionalidad de los elementos involucrados en el proceso de firma digital se ha realizado lo siguiente:

Desde Microsoft Visual Basic se han agregado dos proyectos, un EXE estándar (FirmaDigital) y un DLL ActiveX (Firmar); la idea es que el DLL encapsule los métodos que van a permitir toda la funcionalidad requerida y que éstos sean invocados desde el EXE, para esto desde “FirmaDigital” (EXE) se referencia a “Firmar” (Ver Figura 2).

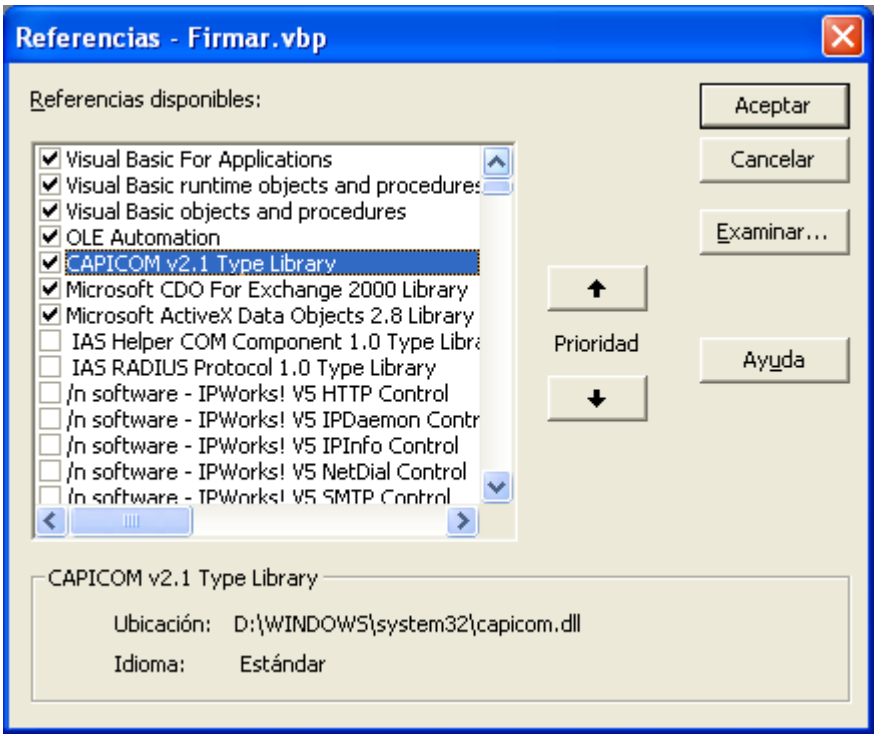
Figura 2: Referencias del EXE



Fuente: Microsoft Visual Basic

En el DLL “Firmar” hay que referenciar a CAPICOM, a CDO para Exchange 2000 y a ADO (ActiveX Data Objects). (Ver Figura 3).

Figura 3: Referencias del DLL



Fuente: Microsoft Visual Basic

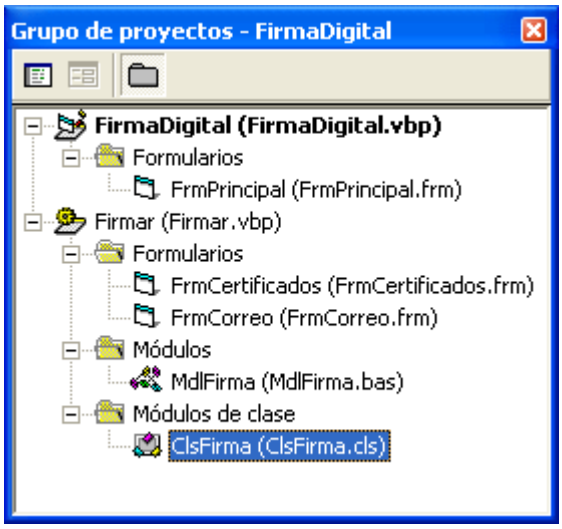
En el caso de CAPICOM para referenciarlo, primero se debe instalar, ya que Microsoft por defecto no incluye este API en sus sistemas operativos, la Plataforma SDK Redistribuible: CAPICOM, está disponible para ser descargada en la dirección download.microsoft.com.

Collaboration Data Objects para Exchange 2000 (CDOEX) es instalado por Microsoft SharePoint Portal Server 2001 (SPS) servidor y cliente y por todas las versiones de Microsoft Office XP. Sin embargo, cualquier código CDOEX que requiera interfases, propiedades y métodos no admitidos por el CDO para Windows 2000 (CDOSYS), un subconjunto de CDOEX, sólo se admite si el código se ejecuta en un equipo con Microsoft Exchange 2000 Server (Microsoft, 2007).

El tercer componente referenciado es ADO, el cual forma parte de Microsoft Data Access Components (MDAC).

Después de hacer las referencias adecuadas, se han agregado cinco objetos al aplicativo; al proyecto ejecutable un formulario llamado FrmPrincipal.frm y al proyecto DLL los formularios FrmCertificados.frm y FrmCorreo.frm, el módulo MdlFirma.bas y la clase ClsFirma.cls en la cual se implementará la mayoría de funciones (Ver Figura 4).

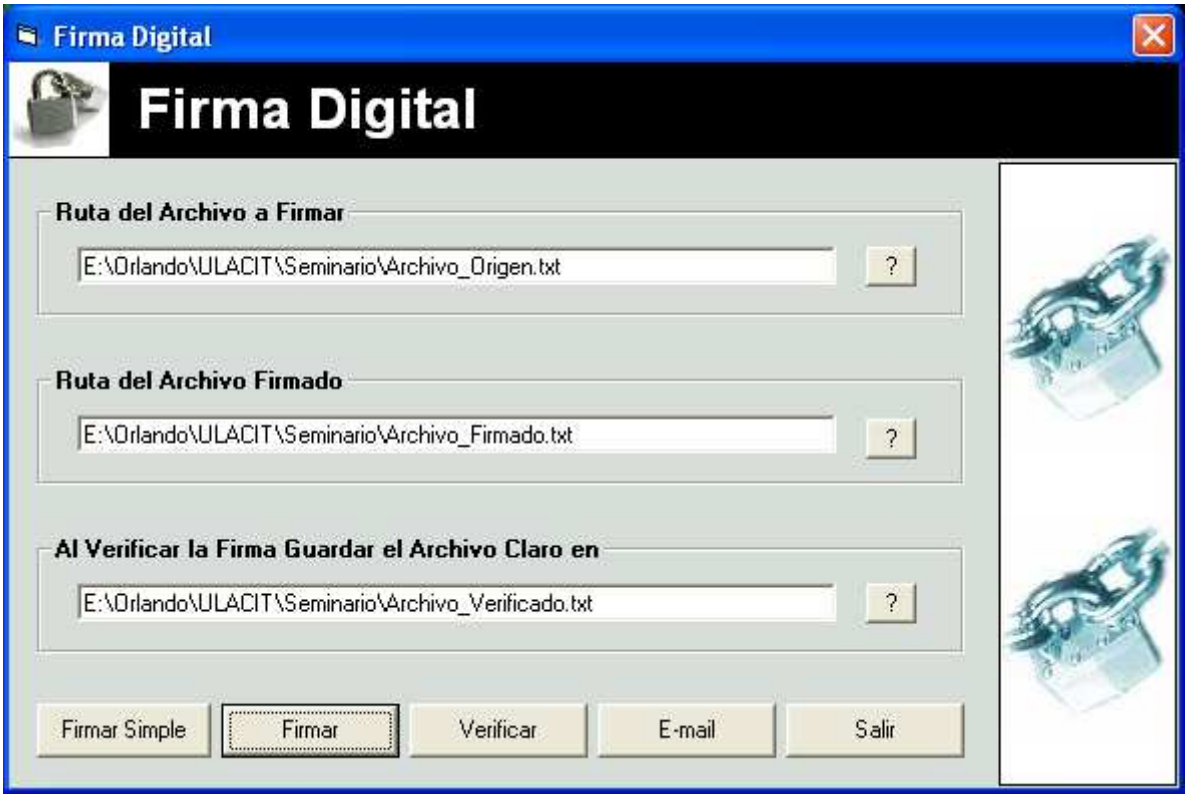
Figura 4: Estructura del Proyecto



Fuente: Elaboración Propia

El formulario FrmPrincipal.frm es la ventana principal de invocación a los procedimientos y funciones provistos por la librería Firmar; esta ventana permite seleccionar el archivo o documento origen por firmar, la ruta donde se creará el archivo firmado digitalmente y la ruta donde se desea que quede el archivo verificado y en claro; a partir de la comprobación del archivo firmado (siempre y cuando la verificación resulte exitosa), la funcionalidad de selección se logra por medio del objeto CommonDialog. La ventana cuenta con botones para firmar y verificar con base en las rutas de trabajo especificadas, además posee un botón independiente para el envío de correo electrónico firmado (Ver Figura 5).

Figura 5: Ventana del EXE



Fuente: Elaboración Propia

El código fuente implementado para la ventana de la figura 5 es el siguiente:

```
Option Explicit
Dim Firma As New ClsFirma

Private Sub Btn_Seleccionar1_Click()
   'Permite especificar la ruta del archivo origen
    CD.DialogTitle = "Selecciona el Archivo a Firmar"
    CD.FileName = "*.txt"
    CD.Filter = "Documentos de texto (*.txt)|*.txt|Todos los archivos|*.*"
    CD.FilterIndex = 1
    CD.ShowOpen
    Txt_Origen = CD.FileName
End Sub

Private Sub Btn_Seleccionar2_Click()
   'Permite especificar la ruta del archivo destino firmado
    CD.DialogTitle = "Ruta del Archivo Firmado"
    CD.FileName = "*.txt"
    CD.Filter = "Documentos de texto (*.txt)|*.txt|Todos los archivos|*.*"
    CD.FilterIndex = 1
    CD.ShowSave
    Txt_Destino = CD.FileName
End Sub
```

```
Private Sub Btn_Seleccionar3_Click()
  'Permite especificar la ruta del archivo verificado
   CD.DialogTitle = "Guardar el Archivo Verificado como"
   CD.FileName = "*.txt"
   CD.Filter = "Documentos de texto (*.txt)|*.txt|Todos los archivos|*.*"
   CD.FilterIndex = 1
   CD.ShowSave
   Txt_Verificado = CD.FileName
End Sub

Private Sub Txt_Origen_GotFocus()
   With Txt_Origen
      .SelStart = 0
      .SelLength = Len(.Text)
   End With
End Sub

Private Sub Txt_Origen_Change()
   If Len(Txt_Origen.Text) > 0 And Len(Txt_Destino.Text) > 0 Then
      Btn_Firmar_Simple.Enabled = True
      Btn_Firmar.Enabled = True
   Else
      Btn_Firmar_Simple.Enabled = False
      Btn_Firmar.Enabled = False
   End If
End Sub

Private Sub Txt_Destino_GotFocus()
   With Txt_Destino
      .SelStart = 0
      .SelLength = Len(.Text)
   End With
End Sub

Private Sub Txt_Destino_Change()
   If Len(Txt_Destino.Text) > 0 And Len(Txt_Origen.Text) > 0 Then
      Btn_Firmar_Simple.Enabled = True
      Btn_Firmar.Enabled = True
   Else
      Btn_Firmar_Simple.Enabled = False
      Btn_Firmar.Enabled = False
   End If
   If Len(Txt_Destino.Text) > 0 And Len(Txt_Verificado.Text) > 0 Then
      Btn_Verificar.Enabled = True
   Else
      Btn_Verificar.Enabled = False
   End If
End Sub

Private Sub Txt_Verificado_GotFocus()
   With Txt_Verificado
      .SelStart = 0
      .SelLength = Len(.Text)
   End With
End Sub
```

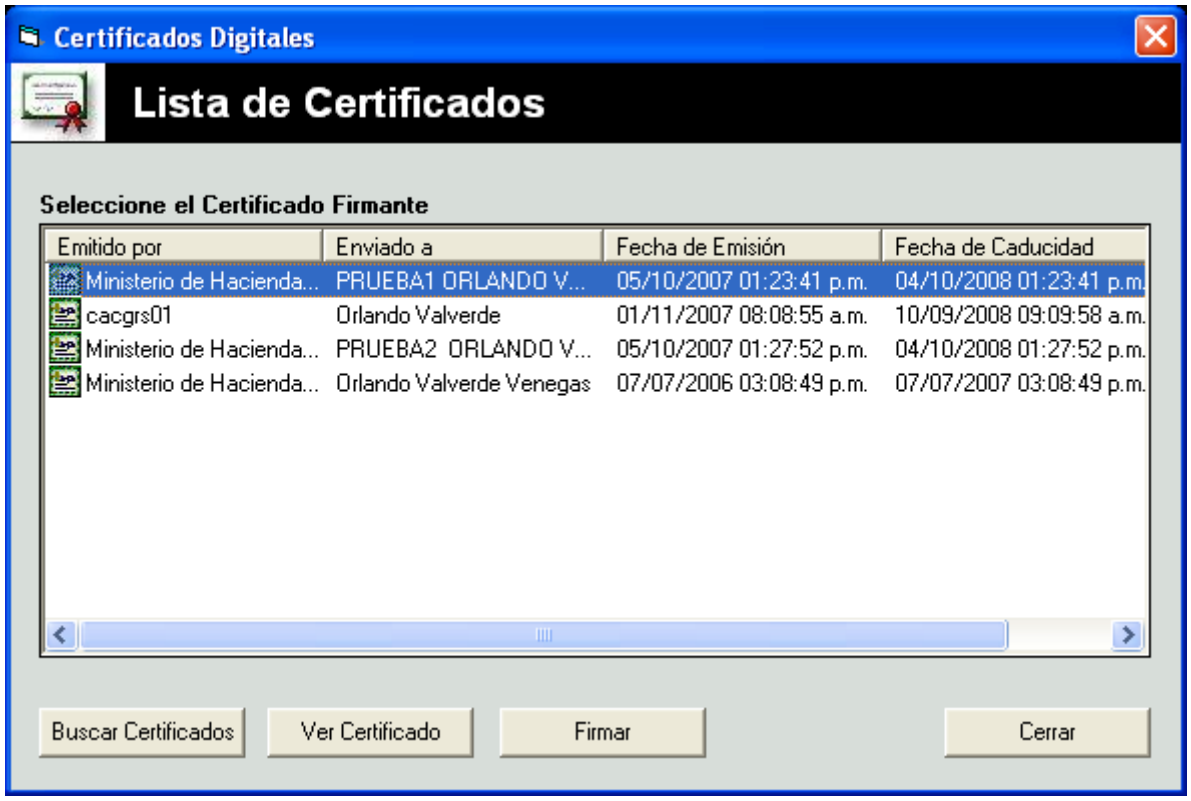
```
Private Sub Txt_Verificado_Change()
   If Len(Txt_Destino.Text) > 0 And Len(Txt_Verificado.Text) > 0 Then
      Btn_Verificar.Enabled = True
   Else
      Btn_Verificar.Enabled = False
   End If
End Sub

Private Sub Btn_Firmar_Simple_Click()
   Firma.Firmar_Simple Txt_Origen.Text, Txt_Destino.Text
End Sub

Private Sub Btn_Firmar_Click()
   Firma.AsignaDatos Txt_Origen.Text, Txt_Destino.Text
   Firma.Selecciona_Firmante
End Sub

Private Sub Btn_Verificar_Click()
   Firma.Verificar Txt_Destino.Text, Txt_Verificado
End Sub

Private Sub Btn_Correo_Click()
   Firma.AsignaServidor
   Firma.Correo_Firmado
End Sub

Private Sub Btn_Salir_Click()
  'Libero recursos utilizados
   Set Firma = Nothing
   End
End Sub
```

La DLL “Firmar” para ejecutar el firmado de archivos provee una ventana que permite buscar y seleccionar el certificado digital por emplear, para lo cual se brinda una lista en modo lectura de todos los certificados encontrados en el almacén de usuario (CAPICOM_CURRENT_USER_STORE), también brinda la opción de ver la información de los certificados (Ver Figura 6).

En el módulo MdlFirma.bas se han agregado tres variables, las dos primeras se cargan a partir de valores pasados por parámetro al invocar el DLL y la tercera se asigna dentro del DLL a partir de un archivo externo que almacena el nombre del servidor de correo por utilizar, el código es el siguiente:

```
Option Explicit
Public Ruta_Origen As String
Public Ruta_Destino As String
Public Servidor As String
```

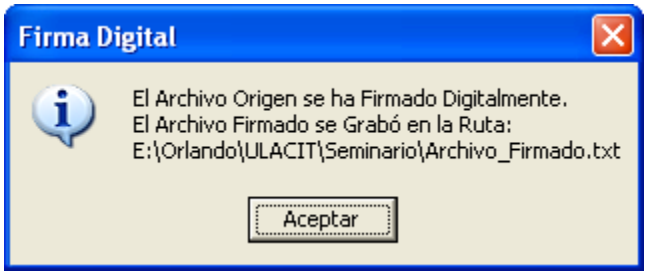
Figura 6: Selecionar Certificado



Fuente: Elaboración Propia

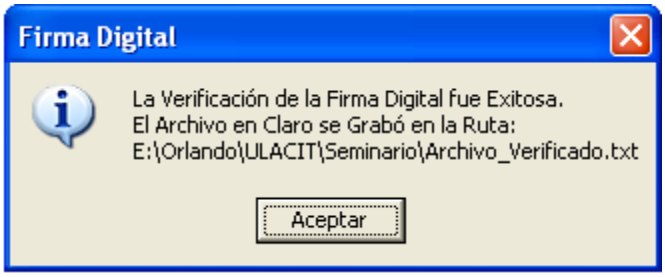
Si el firmado del archivo origen y el verificado del archivo firmado se realizan de forma exitosa, se informa; en caso contrario, se maneja el error mediante el control de excepciones (Ver Figuras 7 y 8).

Figura 7: Firma Exitosa



Fuente: Elaboración Propia

Figura 8: Verificación Exitosa



Fuente: Elaboración Propia

La figura 9 muestra los resultados obtenidos al aplicar el proceso de firmado y verificación. El certificado utilizado está almacenado en un token, por tanto, primeramente se requirió instalar los drivers del dispositivo (proveedor los brinda).

Figura 9: Resultados de Firmar y Verificar

Fuente: Elaboración Propia

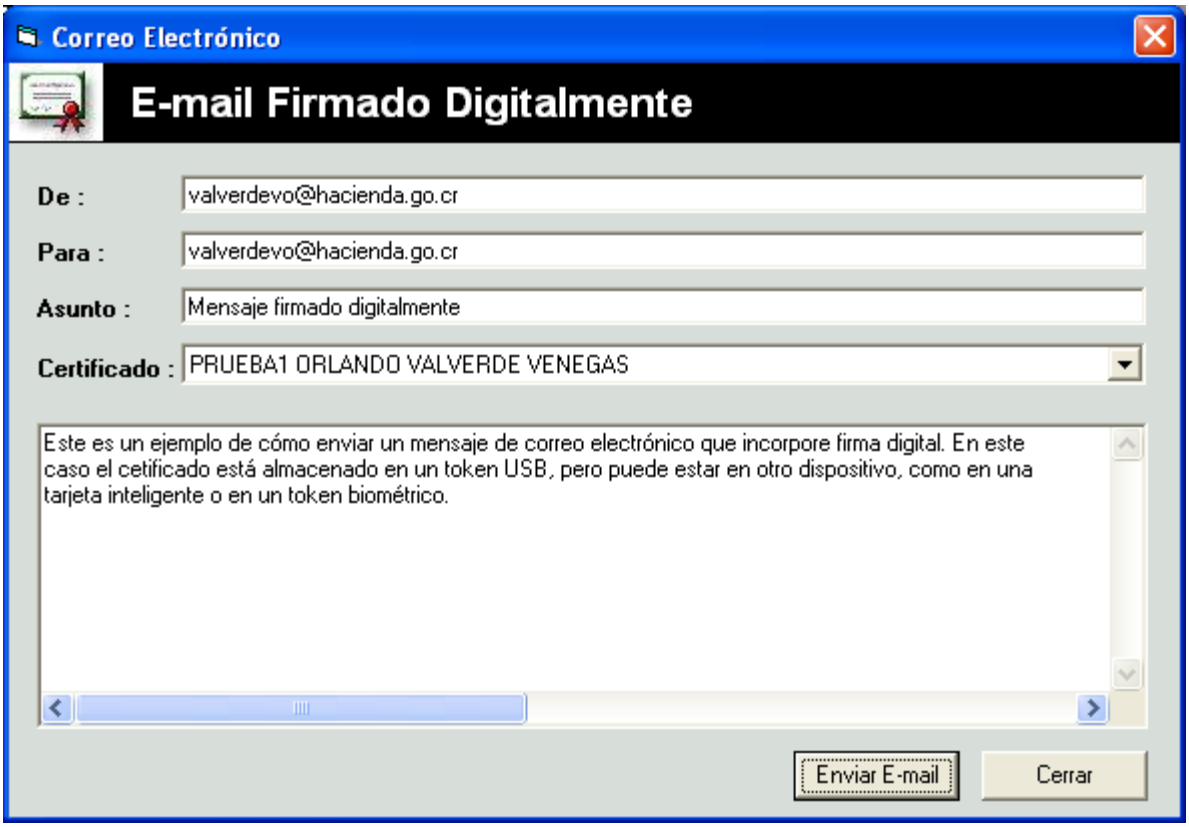
El código fuente utilizado en la ventana de selección del certificado e invocación al método de firma pasando como parámetro el firmante (figura 6), es el siguiente:

```
Option Explicit
Dim Almacen As New CAPICOM.Store    'Objeto almacen de certificados

Private Sub Form_Load()
   Dim clmX As ColumnHeader
   Set clmX = ListView_Certs.ColumnHeaders.Add(, , "Emitido por", ListView_Certs.Width / 3.5)
   Set clmX = ListView_Certs.ColumnHeaders.Add(, , "Enviado a", ListView_Certs.Width / 3)
   Set clmX = ListView_Certs.ColumnHeaders.Add(, ,"Fecha de Emisión", ListView_Certs.Width / 4)
   Set clmX=ListView_Certs.ColumnHeaders.Add(,,"Fecha de Caducidad",ListView_Certs.Width/ 4)
   Set clmX = ListView_Certs.ColumnHeaders.Add(, , "Versión", ListView_Certs.Width / 10)
   ListView_Certs.SmallIcons = ImageList1
End Sub

Private Sub Btn_Buscar_Click()
  'Objeto para acceder al almacén de certificados
   Dim Cert As CAPICOM.Certificate
   Dim li As ListItem
   Dim i As Integer
   ListView_Certs.ListItems.Clear
  'Se abre el almacén de usuario para lectura
   Almacen.Open _
   CAPICOM_CURRENT_USER_STORE, "My", CAPICOM_STORE_OPEN_READ_ONLY
  'Muestra los certificados encontrados
   For i = 1 To Almacen.Certificates.Count
      Set Cert = Almacen.Certificates(i)
      Set li = ListView_Certs.ListItems.Add(, , _
      Cert.GetInfo(CAPICOM_CERT_INFO_ISSUER_SIMPLE_NAME))
      Set li.Tag = Cert
      li.SmallIcon = 1
      ListView_Certs.ListItems(i).ListSubItems.Add , , _
      Cert.GetInfo(CAPICOM_CERT_INFO_SUBJECT_SIMPLE_NAME)
      ListView_Certs.ListItems(i).ListSubItems.Add , , Cert.ValidFromDate
      ListView_Certs.ListItems(i).ListSubItems.Add , , Cert.ValidToDate
      ListView_Certs.ListItems(i).ListSubItems.Add , , Cert.Version
   Next i
  'Libero recursos utilizados
   Set Cert = Nothing
   Set li = Nothing
   ListView_Certs.SetFocus
End Sub

Private Sub ListView_Certs_DblClick()
  'Muestra el certificado seleccionado
   If Not ListView_Certs.SelectedItem Is Nothing Then
      ListView_Certs.SelectedItem.Tag.Display
   End If
End Sub
```

```
Private Sub Btn_Ver_Click()
  'Muestra el certificado seleccionado
   If Not ListView_Certs.SelectedItem Is Nothing Then
      ListView_Certs.SelectedItem.Tag.Display
      ListView_Certs.SetFocus
   End If
End Sub

Private Sub ListView_Certs_ColumnClick(ByVal ColumnHeader As MSComctlLib.ColumnHeader)
   ListView_Certs.SortKey = ColumnHeader.Index - 1
   ListView_Certs.Sorted = True
End Sub

Private Sub Btn_Firmar_Click()
   Dim Cert As CAPICOM.Certificate          'Objeto de certificado
   Dim Firmante As New CAPICOM.Signer  'Objeto firmante
   Dim Fir As New ClsFirma                  'Objeto para Firmar

   If ListView_Certs.ListItems.Count > 0 Then
     'Se obtiene el certificado con el que se va a firmar el mensaje, para
     'ello se extrae el certificado seleccionado por medio de su nombre común
      Set Cert = Almacen.Certificates.Find(CAPICOM_CERTIFICATE_FIND_SUBJECT_NAME, _
      ListView_Certs.SelectedItem.SubItems(1))(1)

     'Se asigna el certificado obtenido al objeto firmante
      Firmante.Certificate = Cert

     'Llamo al procedimiento de firma
      Fir.Firmar Ruta_Origen, Ruta_Destino, Firmante

     'Libero recursos utilizados
      Set Cert = Nothing
      Set Firmante = Nothing
      Set Fir = Nothing

      ListView_Certs.SetFocus
   Else
      MsgBox "Aún no ha Seleccionado un Certificado.", vbCritical, "Firma Digital"
   End If
End Sub

Private Sub Form_Unload(Cancel As Integer)
   Set Almacen = Nothing
End Sub

Private Sub Btn_Cerrar_Click()
   Unload Me
End Sub
```

El DLL implementado también brinda la funcionalidad para firmar correos electrónicos, para ello elaboré una ventana que permite escoger el certificado digital con el cual se firmará el correo saliente, los otros datos por proporcionar son el remitente, destinatario, asunto y el cuerpo del mensaje (Ver Figura 10).

Figura 10: Ventana para enviar Correo Electrónico



Fuente: Elaboración Propia

El token está protegido por una clave para que sólo sea usado por el titular del certificado almacenado, al intentar firmar el mensaje se nos pide que ingresemos la clave. El código fuente de la figura 10 es el siguiente:

```
Option Explicit
Dim Almacen As New CAPICOM.Store     'Objeto almacén de certificados

Private Sub Form_Load()
   'Objeto para acceder al almacén de certificados
    Dim Cert As CAPICOM.Certificate
    Dim i As Integer
   'Se abre el almacén de usuario para lectura
    Almacen.Open _
```

```
    CAPICOM_CURRENT_USER_STORE, "My", CAPICOM_STORE_OPEN_READ_ONLY
   'Llena el combo con los certificados encontrados
    For i = 1 To Almacen.Certificates.Count
       Set Cert = Almacen.Certificates(i)
       Cmb_Certificados.AddItem _
       Cert.GetInfo(CAPICOM_CERT_INFO_SUBJECT_SIMPLE_NAME)
    Next i
   'Libero recursos utilizados
    Set Cert = Nothing
End Sub

Private Sub Btn_Enviar_Click()
   'Permite enviar un mensaje de correo electrónico
    Dim Configuracion As New CDO.Configuration   'Objeto de configuración
    Dim Mensaje As New CDO.Message               'Objeto mensaje de correo
    Dim Cert As CAPICOM.Certificate              'Objeto de certificado
    Dim Firmante As New CAPICOM.Signer           'Objeto firmante
    Dim Fir As New ClsFirma                      'Objeto para Firmar
    On Error GoTo Error

   'Se configura el método de envío de mensajes, nombre del servidor, puerto y el timeout
    Configuracion.Fields.Item("http://schemas.microsoft.com/cdo/configuration/sendusing") = 2
    Configuracion.Fields.Item("http://schemas.microsoft.com/cdo/configuration/smtpserver") = _
    Servidor
    Configuracion.Fields.Item("http://schemas.microsoft.com/cdo/configuration/smtpserverport") = 25
    Configuracion.Fields.Item(http://schemas.microsoft.com/cdo/configuration" + _
    "/smtpconnectiontimeout") = 60
    Configuracion.Fields.Update

   'Se asigna remitente, destinatario, asunto y cuerpo
    Mensaje.From = Txt_De.Text
    Mensaje.To = Txt_Para.Text
    Mensaje.Subject = Txt_Asunto.Text
    Mensaje.HTMLBody = Txt_Mensaje.Text

   'Se obtiene el certificado con el que se va a firmar el mensaje, para
   'ello se extrae el certificado seleccionado por medio de su nombre común
    Set Cert = Almacen.Certificates.Find( _
    CAPICOM_CERTIFICATE_FIND_SUBJECT_NAME, Cmb_Certificados.Text)(1)

   'Se asigna el certificado obtenido al objeto firmante
    Firmante.Certificate = Cert

   'Llamo la función de firma
    Set Mensaje = Fir.Firmar_Correo(Mensaje, Firmante)

   'Se carga la configuración de envío
    Set Mensaje.Configuration = Configuracion

   'Se envía el correo
    Mensaje.Send

   'Libero recursos utilizados
    Set Configuracion = Nothing
    Set Mensaje = Nothing
    Set Cert = Nothing
```

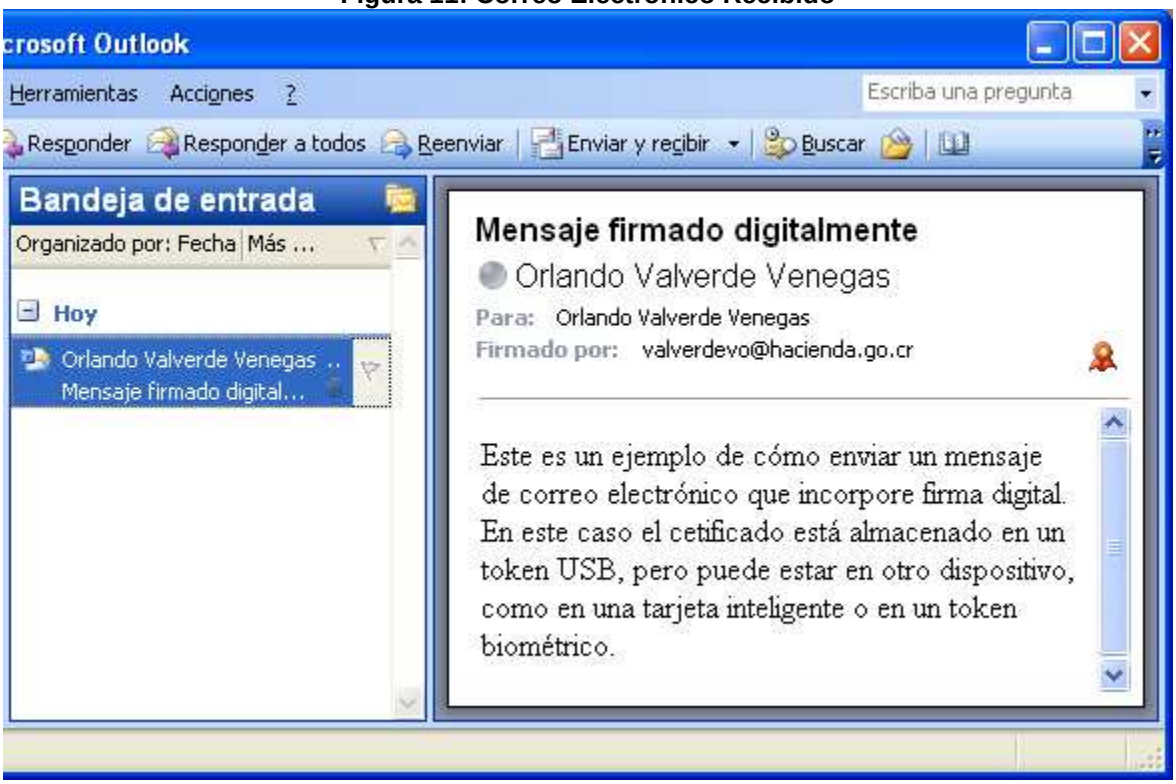
```
    Set Firmante = Nothing

Error:
    If Err.Number <> 0 Then
        MsgBox "Error al Enviar el E-mail: " & Err.Description, vbCritical, "Firma Digital"
    Else
        MsgBox "E-mail Enviado de forma Exitosa.", vbInformation, "Firma Digital"
    End If
End Sub

Private Sub Txt_De_GotFocus()
    With Txt_De
        .SelStart = 0
        .SelLength = Len(.Text)
    End With
End Sub

Private Sub Txt_De_Change()
    If Len(Txt_De.Text) > 0 And Len(Txt_Para.Text) > 0 And Len(Txt_Asunto.Text) > 0 Then
        Btn_Enviar.Enabled = True
    Else
        Btn_Enviar.Enabled = False
    End If
End Sub

Private Sub Txt_Para_GotFocus()
    With Txt_Para
        .SelStart = 0
        .SelLength = Len(.Text)
    End With
End Sub

Private Sub Txt_Para_Change()
    If Len(Txt_De.Text) > 0 And Len(Txt_Para.Text) > 0 And Len(Txt_Asunto.Text) > 0 Then
        Btn_Enviar.Enabled = True
    Else
        Btn_Enviar.Enabled = False
    End If
End Sub

Private Sub Txt_Asunto_GotFocus()
    With Txt_Asunto
        .SelStart = 0
        .SelLength = Len(.Text)
    End With
End Sub

Private Sub Txt_Asunto_Change()
    If Len(Txt_De.Text) > 0 And Len(Txt_Para.Text) > 0 And Len(Txt_Asunto.Text) > 0 Then
        Btn_Enviar.Enabled = True
    Else
        Btn_Enviar.Enabled = False
    End If
End Sub
```

```
Private Sub Form_Unload(Cancel As Integer)
   Set Almacen = Nothing
End Sub

Private Sub Btn_Cerrar_Click()
   Unload Me
End Sub
```

En la figura 11 podemos ver el mensaje enviado ya recibido en la bandeja de entrada de Microsoft Outlook.

Este ícono indica que el mensaje lleva una firma digital válida asociada.

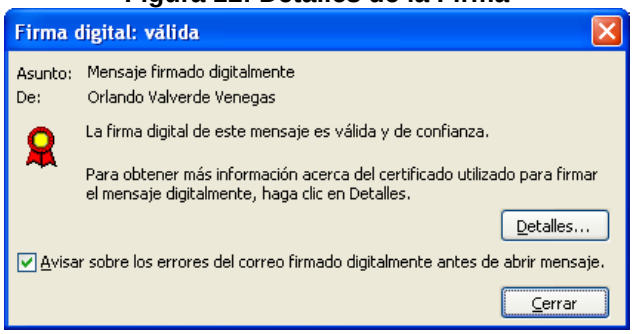
Figura 11: Correo Electrónico Recibido



Fuente: Microsoft Outlook

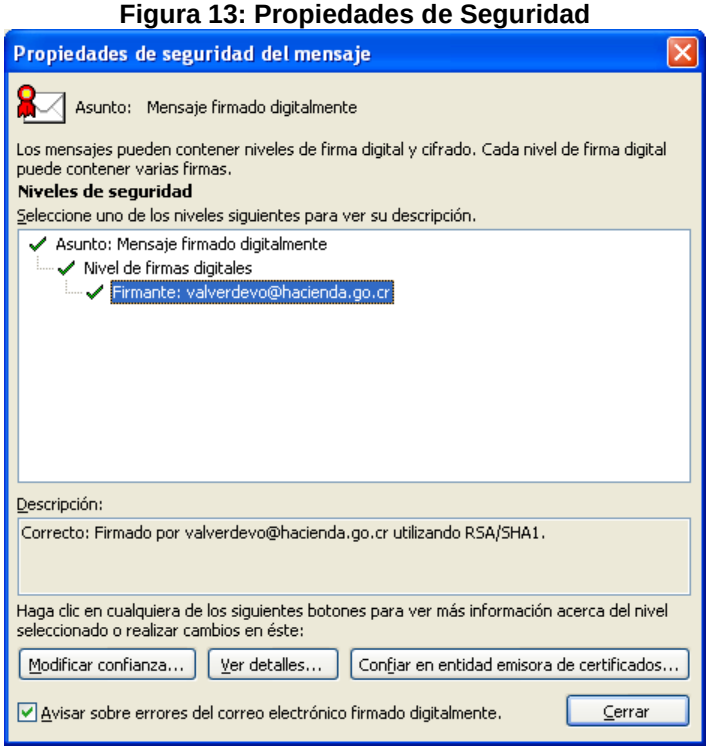
Las figuras 12 y 13 ilustran los detalles del mensaje recibido.

Figura 12: Detalles de la Firma



Fuente: Microsoft Outlook

Figura 13: Propiedades de Seguridad



Fuente: Microsoft Outlook

Es momento de detallar el código fuente de la clase (ClsFirma.cls) que permite las funciones expuestas anteriormente, mediante el uso de certificados digitales.

```
Option Explicit

Public Sub AsignaDatos(Origen As String, Destino As String)
   'Recibe la ruta del archivo a firmar y la ruta donde quedará el archivo firmado
    Ruta_Origen = Origen
    Ruta_Destino = Destino
End Sub
```

```
Public Sub AsignaServidor()
   'Establece el servidor de correo SMTP, en mi caso es: mh-dgi-mail07.mh.hacienda.go.cr
    Servidor = Abrir(App.Path & "\Servidor.txt")
End Sub

Public Sub Firmar_Simple(Origen As String, Destino As String)
   'Recibe la ruta del archivo a firmar y la ruta donde quedará el archivo firmado
    Dim SD As New CAPICOM.SignedData
    Dim Settings As New CAPICOM.Settings
    Dim MsjFirmado As String
    On Error GoTo Error

   'Si el parámetro pSigner es nulo y hay más de un certificado, EnablePromptForCertificateUI
   'se debe establecer en true para que se permita seleccionar el certificado deseado
    Settings.EnablePromptForCertificateUI = True

   'Abro el archivo a firmar
    SD.Content = Abrir(Origen)

   'Firmo el mensaje
    MsjFirmado = SD.Sign(Nothing, False, CAPICOM_ENCODE_BASE64)

   'Libero recursos utilizados
    Set SD = Nothing
    Set Settings = Nothing

Error:
    If Err.Number <> 0 Then
        MsgBox "Error al Firmar: " & Err.Description, vbCritical, "Firma Digital"
    Else
       'Grabo el archivo firmado
        If Grabar(Destino, MsjFirmado) Then
            MsgBox "El Archivo Origen se ha Firmado Digitalmente." + Chr(13) + _
            "El Archivo Firmado se Grabó en la Ruta: " + Chr(13) + _
             Destino, vbInformation, "Firma Digital"
        End If
    End If
End Sub

Public Sub Firmar(Origen As String, Destino As String, Firmante As Signer)
   'Recibe la ruta del archivo a firmar, la ruta donde quedará el archivo firmado y el firmante
    Dim SD As New CAPICOM.SignedData    'Objeto de firma de datos
    Dim MsjFirmado As String
    On Error GoTo Error

   'Abro el archivo a firmar
    SD.Content = Abrir(Origen)

   'Firmo el mensaje utilizando el firmante
    MsjFirmado = SD.Sign(Firmante, False, CAPICOM_ENCODE_BASE64)

   'Libero recursos utilizados
    Set SD = Nothing

Error:
    If Err.Number <> 0 Then
```

```
        MsgBox "Error al Firmar: " & Err.Description, vbCritical, "Firma Digital"
    Else
       'Grabo el archivo firmado
        If Grabar(Destino, MsjFirmado) Then
            MsgBox "El Archivo Origen se ha Firmado Digitalmente." + Chr(13) + _
            "El Archivo Firmado se Grabó en la Ruta: " + Chr(13) + _
             Destino, vbInformation, "Firma Digital"
        End If
    End If
End Sub

Public Sub Verificar(Archivo_Firmado As String, Archivo_Claro As String)
   'Verifica un archivo firmado, si es válido genera un archivo con el contenido original
    Dim SD As New SignedData
    Dim MsjFirmado As String
    Dim MsjOriginal As String
    On Error GoTo Error

   'Abro el archivo firmado
    MsjFirmado = Abrir(Archivo_Firmado)

   'Verifico la firma digital
    SD.Verify MsjFirmado, False, CAPICOM_VERIFY_SIGNATURE_AND_CERTIFICATE

   'Obtengo el contenido original
    MsjOriginal = SD.Content

   'Libero recursos utilizados
    Set SD = Nothing

Error:
    If Err.Number <> 0 Then
        MsgBox "Error al Verificar: " & Err.Description, vbCritical, "Firma Digital"
    Else
       'Grabo un archivo con el contenido original
        If Grabar(Archivo_Claro, MsjOriginal) Then
            MsgBox "La Verificación de la Firma Digital fue Exitosa." + Chr(13) + _
            "El Archivo en Claro se Grabó en la Ruta: " + Chr(13) + _
             Archivo_Claro, vbInformation, "Firma Digital"
        End If
    End If
End Sub

Private Function Abrir(Ruta As String) As String
   'Permite leer el contenido de un archivo secuencial
    Dim FileNum As Integer
    On Error GoTo Error

    FileNum = FreeFile
    Open Ruta For Input As FileNum
    Abrir = Input(LOF(FileNum), FileNum)
    Close FileNum

Error:
    If Err.Number <> 0 Then
        MsgBox "Error de Lectura: " & Err.Description, vbCritical, "Firma Digital"
```

```
    End If
End Function

Private Function Grabar(Ruta As String, Mensaje As String) As Boolean
   'Permite crear un archivo secuencial
    Dim FileNum As Integer
    On Error GoTo Error

    FileNum = FreeFile
    Open Ruta For Output As FileNum
    Print #FileNum, Mensaje
    Close FileNum

Error:
    If Err.Number <> 0 Then
        Grabar = False
        MsgBox "Error al Grabar: " & Err.Description, vbCritical, "Firma Digital"
    Else
        Grabar = True
    End If
End Function

Public Function Firmar_Correo(Mensaje As Message, Firmante As Signer) As Message
   'Permite firmar un mensaje de correo
    Dim SD As New CAPICOM.SignedData    'Objeto de firma de datos
    Dim SegMensaje As New CDO.Message  'Objeto de mensaje que será firmado
    Dim Stream As New ADODB.Stream         'Objeto para el volcado de los datos firmados
    Dim CuerpoMsj As String
    Dim DatosFirmados As String
    Dim Cabecera
    On Error GoTo Error

   'Se carga el contenido del mensaje original
    SegMensaje.DataSource.OpenObject Mensaje, "IMessage"

   'Se configuran las cabeceras del mensaje
    Set Cabecera = SegMensaje.BodyPart
    Cabecera.ContentMediaType = _
    "application/pkcs7-mime;smime-type=signed-data;name=smime.p7m"
    Cabecera.ContentTransferEncoding = "base64"
    Cabecera.Fields("urn:schemas:mailheader:content-disposition") = _
    "attachment;FileName=""smime.p7m"""
    Cabecera.Fields.Update

   'Se extrae el cuerpo del mensaje
    CuerpoMsj = Mensaje.BodyPart.GetStream.ReadText

   'Se asigna el cuerpo del mensaje convertido en ASCII
    SD.Content = Unicode_Ascii(CuerpoMsj)

   'Firmo el mensaje utilizando el firmante recibido por parámetro
    DatosFirmados = SD.Sign(Firmante, False, CAPICOM_ENCODE_BASE64)

   'Se obtiene el Stream que corresponde al cuerpo del mensaje
    Set Stream = SegMensaje.BodyPart.GetEncodedContentStream
    Stream.Type = adTypeText
```

```
   'Se vuelcan en el Stream los datos firmados
    Stream.WriteText DatosFirmados
    Stream.Flush

   'Devuelvo el mensaje firmado
    Set Firmar_Correo = SegMensaje

   'Libero recursos utilizados
    Set SD = Nothing
    Set SegMensaje = Nothing
    Set Stream = Nothing
    Set Cabecera = Nothing

Error:
    If Err.Number <> 0 Then
        MsgBox "Error al Firmar el E-mail: " & Err.Description, vbCritical, "Firma Digital"
    End If
End Function

Private Function Unicode_Ascii(Unicode As String) As String
   'Convierte una cadena Unicode a ASCII
    Dim Largo, J, NumAscii As Long
    Dim CadenaAscii As String
    Largo = Len(Unicode)
    For J = 1 To Largo
        NumAscii = Asc(Mid(Unicode, J, 1))
        CadenaAscii = CadenaAscii & ChrB(NumAscii)
    Next
    Unicode_Ascii = CadenaAscii
End Function

Public Sub Selecciona_Firmante()
    FrmCertificados.Show 1
End Sub

Public Sub Correo_Firmado()
    FrmCorreo.Show 1
End Sub
```

Material de apoyo: (Microsoft, 2007), (Kachroo, N, 2000), (Alvarez, G, 2006), (Lambert, J, 2001).

V. Conclusiones

En esencia, el concepto de firma digital no dista mucho de la firma convencional o manuscrita; en donde sí hace notable diferencia es en el nivel de seguridad que brinda a la información, lo cual permite reducir tiempos al brindar la posibilidad de tramitar documentación certificada, vía correo electrónico.

Se hizo alusión a una serie de términos y conceptos ligados con el uso de certificados y firmas digitales a nivel conceptual; posteriormente profundizamos en el desarrollo técnico de un aplicativo para respaldar la teoría planteada. Se mostró cómo firmar y el formato interno que contiene un archivo firmado digitalmente y cómo a partir de éste se puede verificar la firma y obtener la información original si el archivo no ha sido alterado. Hemos visto cómo software de correo electrónico comercial (Outlook) valida, muestra y brinda información relevante en relación con la mensajería firmada digitalmente, de manera que el trasiego de documentación que incluye firmado digital resulta fácil y transparente para el usuario final.

Además, se ha podido demostrar lo sencillo y cómodo que es acceder a funciones criptográficas avanzadas, mediante el uso de CAPICOM para el firmado y verificación de archivos y lo valiosas que resultan estas funciones combinadas con un componente que permita la administración de mensajería como CDO. Por ende, los objetivos planteados al inicio de este artículo se han alcanzado y tanto los pasos necesarios como la totalidad del código fuente comentado y sus pruebas, han quedado claramente expuestos.

Sin duda alguna, la firma digital es una herramienta tecnológica que hace y hará diferencia en una sociedad cada vez más digitalizada, en donde la transferencia de información en formato digital acapara prácticamente cualquier sector concebido.

Referencias Bibliográficas

Alvarez, G. (2006). *Envío de mensajes cifrados y firmados desde ASP/IIS Cómo utilizar CAPICOM para proteger mensajes de correo desde páginas web.* Recuperado el 13 de octubre de 2007, de http://www.idg.es/pcworld/index.asp?link=estructura/i_articulo_centroArticulo.asp&IdArticulo=173235

CA Banesto. (2007). *S/MIME.* Recuperado el 22 de noviembre de 2007, de http://ca.banesto.es/ayuda/faqs/imprime/faq3.html

Cea, A.J. (2000). *El algoritmo RSA *YA* es de dominio público.* Recuperado el 05 de noviembre de 2007, de http://www.hispasec.com/unaaldia/698

Hess, A.C. (2007). *Taller sobre implicaciones jurídicas de la firma Digital.* Recuperado el 13 de noviembre de 2007, de http://www.hess-cr.com/secciones/dere-info/index.shtml#otros

Kachroo, N. (2000). *Guía básica de los objetos de datos de colaboración.* Recuperado el 13 de octubre de 2007, de http://msdn.microsoft.com/library/spa/default.asp?url=/library/SPA/dntaloc/html/cdo_roadmap.asp

La Gaceta. (2006). *Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos.* Recuperado el 13 de noviembre de 2007, de http://www.hess-cr.com/secciones/dere-info/index.shtml#otros

Lambert, J. (2001). *Introducing CAPICOM.* Recuperado el 01 de octubre de 2007, de http://msdn2.microsoft.com/en-us/library/ms995332.aspx#intcapicom_int

Ley 8454. (2005). *Ley de Certificados, Firmas Digitales y Documentos Electrónicos.* Recuperado el 13 de noviembre de 2007, de http://www.hess-cr.com/secciones/dere-info/index.shtml#otros

Llorente, I.M. (2006). *Introducción a la Seguridad en un Grid.* Recuperado el 12 de octubre de 2007, de www.fdi.ucm.es/profesor/rubensm/Doctorado/Introduccion%20a%20la%20Seguridad%20en%20un%20Grid.pdf

Lucena, L.M. (2003). *Criptografía y Seguridad en Computadores.* Recuperado el 06 de octubre de 2007, de www.uned.es/413042/material/Criptografia.pdf

Marrero, T.Y. (2006). *La Criptografía como elemento de la seguridad informática.* Recuperado el 23 de octubre de 2007, de http://web.ebscohost.com/ehost/detail?vid=1&hid=113&sid=29a74ea6-8a35-41cb-ac01-6d79be99e2ad%40sessionmgr109

Microsoft. (2006). *Apéndice 4: Claves y certificados.* Recuperado el 03 de octubre de 2007, de http://www.microsoft.com/spanish/msdn/arquitectura/BuildSecNetApps/html/Appendix_04.mspx

Microsoft. (2007). *CAPICOM Reference.* Recuperado el 29 de setiembre de 2007, de http://msdn2.microsoft.com/en-us/library/Aa375732.aspx

Microsoft. (2007). *CDOEX Is Installed by Office XP, SharePoint Portal Server, and Client.* Recuperado el 20 de octubre de 2007, de http://support.microsoft.com/kb/319105/en-us

Microsoft. (2007). *MS07-028: Una vulnerabilidad en CAPICOM podría permitir la ejecución remota de código.* Recuperado el 08 de octubre de 2007, de http://support.microsoft.com/kb/931906/es

Universidad de Murcia. (1999). *Documento sobre incorporación de certificados en el Directorio.* Recuperado el 20 de octubre de 2007, de http://www.um.es/redes/x500/isode4/iris-search-9905-03.html

Universidad de Murcia. (2007). *La seguridad en informática.* Recuperado el 25 de octubre de 2007, de http://www.um.es/docencia/barzana/IAGP/Iagp10.html#BM5

Villalón, H.A. (2006). *Seguridad en Unix y redes.* Recuperado el 06 de octubre de 2007, de http://www.wikilearning.com/criptosistemas_de_clave_publica-wkccp-9777-117.htm

Wikipedia. (2007). *SHA.* Recuperado el 01 de noviembre de 2007, de http://es.wikipedia.org/wiki/SHA