C A P Í T U L O V

ESTUDIO DE LA PLATAFORMA

5.1 Estudio de Requerimientos

5.2 Sistema Operativo Windows 2000 Server

5.3 Visual Basic.NET

5.1 Estudio de Requerimientos

Para el desarrollo del Aplicativo Notaría Digital, bajo Windows 2000 Server y Microsoft Visual Basic.NET, es necesario contar con los siguientes requisitos y configuraciones:

Windows 2000 Server con Service Pack 2 o posterior, instalado y configurado, bajo un controlador de Dominio.

Internet Information Server IIS, instalado y configurado

SQL Server 7.0 o Posterior, para el Aplicativo se ha escogido SQL Server 2000, instalado y configurado.

.NET Framework 1.1 y Visual Basic.NET Versión 2003 en Español, instalados y configurados

Internet Explorer 6.0, para el correcto funcionamiento de la aplicación además de **ASP.NET**

5.2 Sistema Operativo Windows 2000 Server

Windows 2000 Server, es un Sistema Operativo que ofrece múltiples ventajas, respecto de otros para establecer mecanismos de seguridad a nivel de acceso de usuarios y acceso a las aplicaciones

Es necesario contar con la configuración adecuada que permita el óptimo desenvolvimiento y rendimiento de la aplicación Notaría Digital.

Las características esenciales que reúne Windows 2000 Server para el desarrollo de este Aplicativo son:

- Es un Sistema Operativo ideal para Servidores
- Alto nivel de Administración de acuerdo a las necesidades

- Facilidad de Configuración del Servidor
- Fácil Administración y Seguridad a Nivel de Directorio de Windows

Las ventajas que ofrece la herramienta Internet Information Server, constituyen la mejor manera de configurar el Servicio Web para la aplicación, la misma que tiene un directorio Virtual NOTARIADIGITAL, en donde residen los archivos necesarios para la página Web.

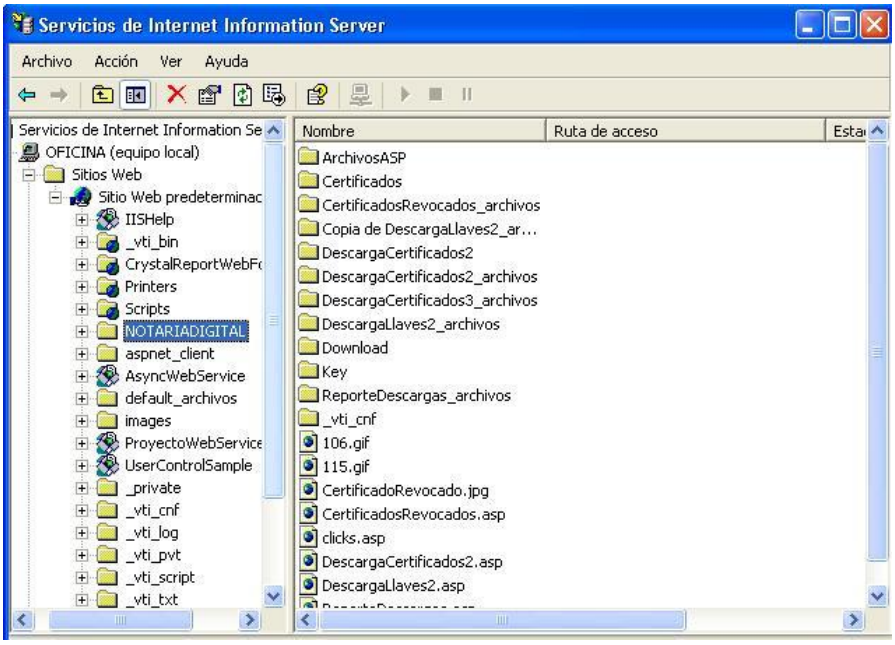

Figura 51 Área de Configuración de Servicios IIS

Cifrado seguro en Windows.- las versiones de Windows 2000 Server con Service Pack 1 o anterior, no permiten la implementación de cifrado, .NET Framework, necesita High Encryption Pack. Que viene incluido desde Service Pack 2 para Windows 2000. Para Windows NT® 4.0, se distribuyen Service Packs tanto en versiones estándar como de cifrado de alto nivel. Service Pack 6ª de Alto Nivel es la Solución adecuada.

Para Windows ME, Windows 98 y Windows 95, Microsoft Internet Explorer 5.5 incluye High Encryption Pack. Si ejecuta una versión de

Internet Explorer anterior a la 5.5, se puede obtener el paquete High Encryption Pack correspondiente.

5.3 Visual Basic.NET

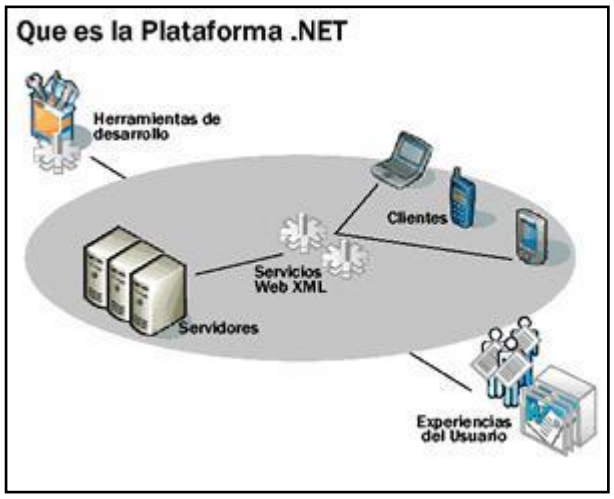

Figura 52 Plataforma .NET

La Plataforma de desarrollo NET FRAMEWOR, y VISUAL STUDIO .NET, son lo último en tecnología de desarrollo de Microsoft, con una gran capacidad y Flexibilidad para el desarrollo de Aplicaciones Orientadas a Objetos, con un entorno de desarrollo integrado y de fácil manejo que ofrecen una gran Escalabilidad y Acoplamiento, por lo que se ha escogido la Herramienta de Visual Basic .NET, como Lenguaje de Programación.

Figura 53 Marco de Trabajo de .NET

El enorme auge en el crecimiento del Comercio Electrónico subraya la necesidad de salvaguardar la privacidad de los datos. Microsoft® trató por primera vez la cuestión de la privacidad de los datos en 1996 con la introducción de Cryptography API (Crypto API). En la actualidad, la constante evolución que ha experimentado la seguridad se centra en el desarrollo de los servicios criptográficos como el espacio de nombres **System.Security.Cryptography** de Microsoft .NET Common Language Runtime (CLR). Este espacio de nombres permite el acceso mediante programación a una gran variedad de servicios criptográficos que puede integrar para cifrar y descifrar datos, garantizar la seguridad de los mismos, así como controlar las firmas y certificados digitales. Algunos de estos servicios se utilizan en otras partes de Framework como la autenticación de ASP.NET.

El espacio de nombres **Cryptography**, es el nivel más alto, se puede separar en cuatro divisiones principales.

1. **Algoritmos de cifrado.-** Conjunto de clases utilizado para implementar cifrados tanto simétricos como asimétricos y algoritmos hash.
2. **Clases Helper.-** Clases utilizadas para generar números aleatorios, efectuar conversiones, interactuar con el almacén Crypto API y realizar los cifrados en sí con un modelo basado en secuencias.
3. **Certificados X.509.-** Clases definidas en el espacio de nombres System.Security. Cryptography.X509Certificates utilizadas para representar certificados digitales.
4. **Firmas digitales XML.-** Clases definidas en el espacio de nombres de System. Cryptography.Xml utilizadas para representar firmas digitales en

Figura 5.4 Librerías de Clases .NET

La función principal del espacio de nombres Cryptography consiste en proporcionar clases que implementen algoritmos para elementos tales como el cifrado y la creación de valores hash. Estos algoritmos se implementan mediante un modelo extensible formado por dos niveles de herencia. Una clase base abstracta como AsymmetricAlgorithm o HashAlgorithm se sitúa en la parte superior de la jerarquía e indica el tipo de algoritmo. Una clase abstracta de segundo nivel se deriva entonces de la clase de nivel superior para proporcionar la interfaz pública para el algoritmo. Por ejemplo, la clase SHA1 se deriva de HashAlgorithm y contiene métodos y propiedades particulares del algoritmo SHA1. Por último, la implementación del algoritmo se deriva del segundo nivel y es desde ahí donde se crea la instancia que utilizan las aplicaciones cliente. En este nivel concreto, las implementaciones se pueden administrar, no administrar, o bien realizar ambas acciones.

Las aplicaciones no administradas normalmente contienen el sufijo "CryptoServiceProvider", por ejemplo SHA1CryptoServiceProvider, para indicar que la implementación la proporciona en realidad el proveedor de servicios de cifrado (CSP) que se instala en el nivel del sistema operativo y actúa como contenedor alrededor de Crypto API. Las implementaciones administradas contendrán el sufijo "Managed",

como en SHA1Managed, no se basarán en Crypto API y, por tanto, se implementarán totalmente en código administrado.

La colección de clases del espacio de nombres **System. Security.Cryptography** incluye clases utilizadas durante el proceso de cifrado/descifrado de datos, así como varias clases auxiliares. El espacio de nombres contiene clases abstractas como, RandomNumberGenerator de la que se deriva, NGCryptoServiceProvider y las clases ToBase64Transform y FromBase64Transform utilizadas para transformar datos de y desde Base 64.
Además de exponer algoritmos criptográficos, el espacio de nombres Cryptography también contiene el espacio de nombres secundario X509Certificates. Éste contiene sólo tres clases utilizadas para representar y administrar los certificados de Authenticode X.509 v.3. La clase X509Certificate expone los métodos estáticos CreateFromCertFile y CreateFromSignedFile para crear una instancia del certificado.

Además .NET Framework permite implementaciones de cualquier otro algoritmo de cifrado, hashing o firma digital a través de propias funciones realizadas por el programador así como también Dll's generadas a partir de algoritmos creados en otros lenguajes de programación.