COMUNICACIONES DOCUMENTALES EN LA ADMINISTRACION DE JUSTICIA.

En el marco de la implementación de un **Plan de Choque para la Agilización de la Administración de Justicia** y según texto de la intervención del Excmo. Ministro de Justicia D. Angel Acebes Paniagua ante la Comisión de Justicia e Interior en el Congreso, extraemos el siguiente párrafo:

"Lo que ahora tarda meses podría hacerse en horas con la ***implantación de un sistema de interconexión*** de los órganos jurisdiccionales entre sí y con los profesionales del Derecho. Los Tribunales podrán por esta vía dirigirse exhortos, notificar resoluciones a los Procuradores, recabar información necesaria para el proceso de los Registros Públicos o recibir documentos electrónicos con eficacia procesal. Si tenemos en cuenta que las comunicaciones *suponen hasta el 30% de las dilaciones procesales* podemos concluir que el nuevo sistema de comunicación agilizará extraordinariamente el servicio público de la Justicia."

Con estas miras se propone en la Subdirección de Informática perteneciente al Ministerio de Justicia, el proyecto piloto **LexNeT** , que sirva como experiencia para la intercomunicación de documentos entre todos los operadores jurídicos y los órganos Judiciales, con características de un sistema abierto que posibilite en ultima instancia la comunicación de los ciudadanos con la Administración de Justicia.

ANTECEDENTES.

Apoyándonos en el Estudio de la Seguridad en las "Comunicaciones Informáticas de los Órganos Jurisdiccionales en España" elaborado por el Consejo General del Poder Judicial y en la experiencia piloto sobre mensajería segura en la Audiencia Nacional Contencioso, vimos que, como primer paso en la elección de la solución, debíamos elegir entre el modelo de mensajería o el modelo de WEB.

Inicialmente el modelo de mensajería, junto a una **Autoridad de Certificación** externa, nos garantizaba en un entorno abierto, tanto sobre redes privadas existentes como por la propia Internet, determinadas características que necesitaba nuestro sistema:

Integridad, autenticidad y confidencialidad entre los documentos intercambiados.

Sin embargo dado el actual sistema abierto de los MTA's del correo de Internet, que por otro lado ha posibilitado su tremenda expansión, no le podríamos requerir a estos sistemas, otras características que necesitaríamos posteriormente, tales como el "no repudio en recepción", "marcas de tiempo" etc, sin la necesidad de tener que intervenir en los sistemas finales de los usuarios o en los MTAS implicados en el proceso.

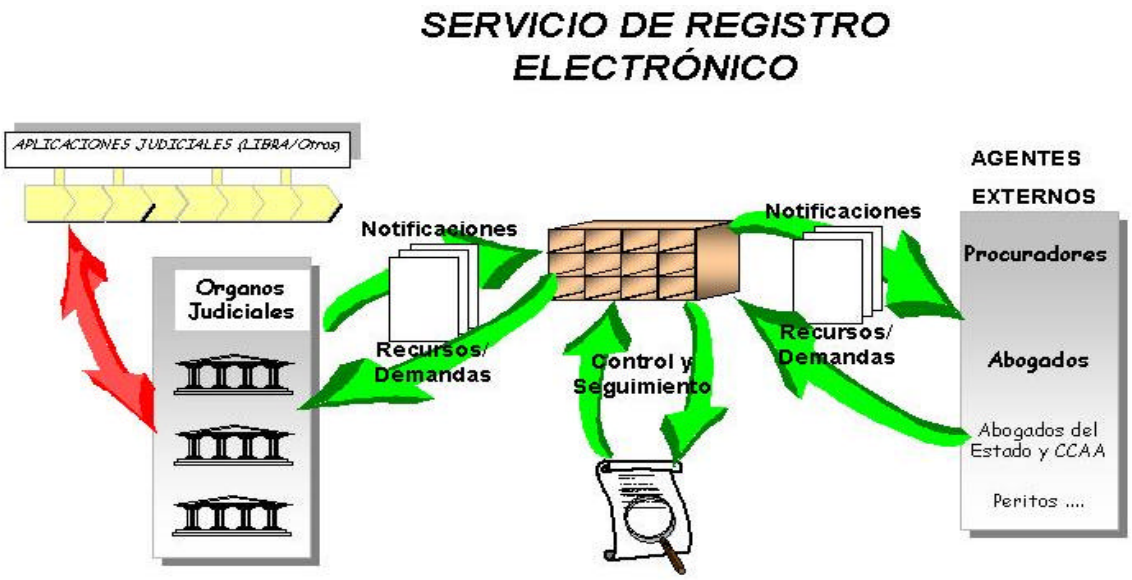
Con la premisa de la menor intervención posible en los sistemas finales de los usuarios y de cara a situarnos en un marco que posibilitase añadir características como las indicadas anteriormente, nos decidimos por una arquitectura de **WEB seguro**, donde poder garantizar las exigencias del intercambio de documentos en el ámbito de la Administración de Justicia.

MISIÓN del proyecto LexNet.

Desarrollar un Piloto de Intercomunicación entre determinados Órganos Judiciales y los Procuradores. Realizando un proyecto real y acotado que posibilite la interconexión a través de Internet de los operadores Jurídicos, de modo que se evalúen todos y cada uno de los conceptos relacionados con la utilización de medios telemáticos, transacciones y tramitación electrónica y en especial los referidos a la seguridad.

OBJETIVOS del proyecto LexNet.

El objetivo del proyecto es la creación de un **Servicio de Registro Electrónico** concretado en las relaciones externas de los Juzgados y Procuradores.



El cual debe cumplir con características de:

1) Identificación de los interlocutores.
2) Protección de los datos de revelaciones no autorizadas.
3) Garantizar la inalterabilidad de los documentos.
4) Evitar el no repudio tanto en envío como en recepción.
5) Certificar los tiempos de entrega como de recogida.
6) Posibilitar la comunicación en cualquier hora y día del año.

Todas las características indicadas anteriormente, para su implementación en un entorno abierto, necesitan del soporte tecnológico de una criptografía de clave pública gestionada mediante **PKI,** utilizando una **Autoridad de Certificación** externa al sistema, lo que nos abocan a nuestro siguiente objetivo:

Evaluar los sistemas de seguridad referidos a la firma electrónica, encriptación, autentificación y certificación incluyendo sistemas avanzados de certificación, tales como notaría electrónica, certeza de no repudio en recepción y sellado del tiempo en documentos.

Para este piloto, se prestará especial atención a la evaluación de todas las sinergias con el proyecto **CERES**.

ESTRATEGIA.

Para que la realización del piloto sea extensible con posterioridad a su implantación real, deberemos utilizar:

1)**Tecnologías estándar** basadas en Internet, que permiten una escalabilidad de la solución.

2)**Soluciones sencillas**, que impliquen el menor numero de componentes en el puesto de trabajo, tales como un Navegador y tarjeta con claves.

3)**Soluciones globales**, que permitan integrar a Comunidades Autónomas con competencias de Justicia, Abogados, Ministerios y otros Organismos Oficiales y en ultima instancia al propio ciudadano.

4)**Soporte Legal**

Ley 30/1992 de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Real Decreto 263/1996 de 16 de febrero, regulador de la utilización de las técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado

Ley 66/1997 de 30 de diciembre, de Medidas Fiscales Administrativas y del Orden Social.

Real Decreto 1290/1999 de 23 de julio, por el que se desarrolla el artículo 81 de la Ley 66/1997 de 30 de diciembre.

Real Decreto-Ley Firma Electrónica 14/1999 de 17 de septiembre.

Reglamento de acreditación de prestadores de servicios de certificación. Orden de 21 de Febrero 2000.

Directiva Europea, Noviembre 99.

PROYECTO LEXNET

Modelo.

El núcleo del sistema del Servicio de Registro Electrónico se basa en un WEB seguro, donde se realizarán las transacciones documentales y que se adapta aun modelo de Seguridad de **WEB Gestionado** con las siguientes posibilidades:

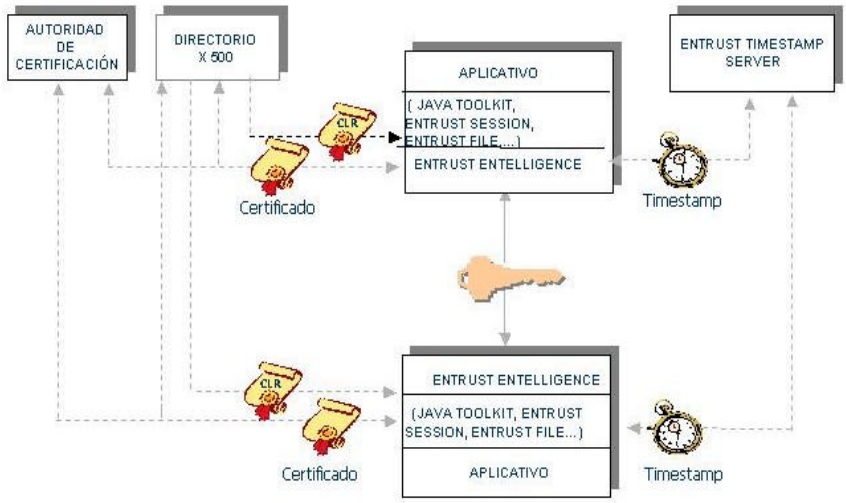
1) Cifrado de documentos.
2) Utilización de firmas digitales.
3) Sellado de tiempo.
4) Soporte de APIs estándar para cualquier aplicación.
5) Chequeo automático de Certificados Revocados.
6) Recuperación de Clave Privada de Descifrado.
7) Renovación Automática de Claves,
8) Gestión del histórico de Claves Privadas de descifrado.
9) Soporte de No Repudio.
10) Soporte de Certificación Cruzada.

11) Gestión transparente del contenedor de claves.
12) Movilidad de los usuarios de un sistema a otro.
13) Política de seguridad definida por el administrador de seguridad.

Componentes.

Los *componentes funcionales* del sistema están ubicados en los servicios de la PKI, el WEB seguro y los puestos de trabajo tal como se indica a continuación:

MODELO FUCIONAL



Los *componentes físicos* del sistema, integrados en la Red de la Administración de Justicia o en un acceso a la red de Internet, están formados por:

Un **servidor,** donde se encuentra la propia aplicación de transacción de documentos, y que tiene como tareas:

1)Almacenar las notificaciones en los buzones.
2)Gestionar accesos y permisos.
3)Registrar tiempos.
4)Registrar transacciones de remisión.
5)Consultar estado de remisiones
6)Certificar y Verificar firmas(coordinado con la CA).

Puestos de trabajo (PCs) con dispositivo de lector de tarjeta, software de Navegador y software de la PKI.

De estos distinguiremos el puesto del **Órgano Judicial**, para Jueces y Secretarios, que se encuentra integrado en el Sistema de Información del Juzgado. Para el piloto se realizará un interfaz con la **Aplicación Libra** existente en todos los Órganos Judiciales que atiende el Ministerio de Justicia. Las tareas de este puesto de trabajo se concretan en:

1)Autentificación de Juez o Secretario.
2)Autentificación del órgano.
3)Firma de documentos.
4)Cifrado en su caso.
5)Envío y registro de estos.
6)Consulta de envíos.
7)Recepción de documentos.

El otro tipo de puesto de trabajo corresponde al **Procurador,** con las tareas de:

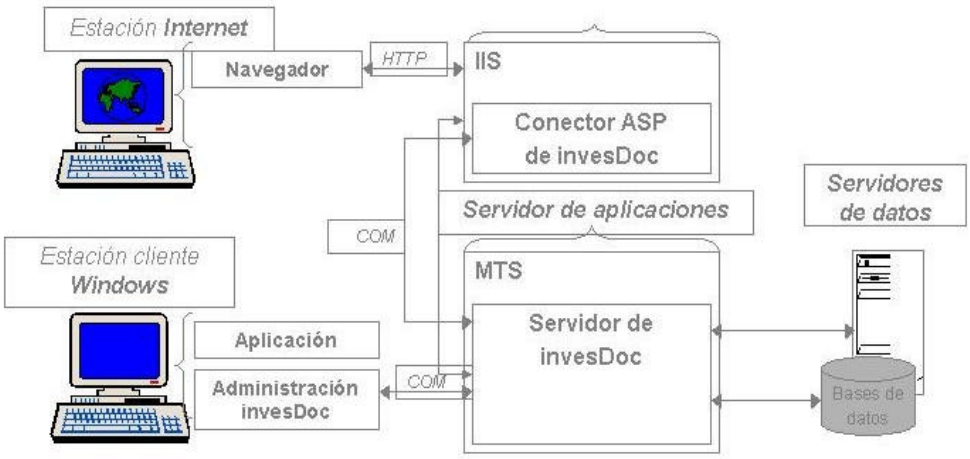
1)Recoger notificaciones.
2)Descifrar en su caso.
3)Comprobar firma.
4)Realizar envíos.
5)Recoger certificados de envíos.

Arquitectura del Sistema.

La arquitectura del sistema elegida para el proyecto, se basa en el modelo de los tres niveles, cliente Navegador, Servidor de Aplicaciones Web y Servidores de Datos, y para el piloto se ubicarán en un solo equipo los componentes de servidor de Aplicaciones y Servidor de Base de Datos.

Las distintas componentes tecnológicas que se han optado para el proyecto piloto, vienen indicadas en el siguiente gráfico:

Arquitectura del Sistema



Conclusiones.

Elaborada la experiencia piloto, ¿que deberemos obtener del trabajo realizado?. Lo podemos resumir en:

1) Agilidad en la comunicación de la información.
2) Seguridad en la recepción de documentos (canales seguros, mucho más que en el proceso manual).
3) Confidencialidad extremo a extremo.
4) Autentificación del emisor(certeza de la firma electrónica).
5) Integridad de la información(cualquier manipulación o cambio por mínima que sea es detectada).
6) Herramientas de medición de la eficiencia del proceso.
7) Extrapolación de la solución de manera inmediata, lineal y funcional.