JUNTA DE ANDALUCIA

IMPLANTACIÓN DE LA FIRMA ELECTRÓNICA EN LA ADMINISTRACIÓN DE JUSTICIA EN ANDALUCÍA.

Autores:

- Julio Úbeda Gea. Jefe de Servicio de Informática Judicial. Consejería de Justicia y Administración Pública. Junta de Andalucía.
  Tlf.:955 043 187/293
  e-mail:jubeda@cgob.dgraj.junta-andalucia.es
- Juan Gasch Illescas. Técnico de Sistemas. Consejería de Justicia y Administración Pública. Junta de Andalucía.
  Tlf.:955 043 188
  e-mail:jgasch@cgob.dgraj.junta-andalucia.es

Punto del temario al que se refiere:

- Infraestructura tecnológica en materia de seguridad para las transacciones con las Administraciones Públicas.

Resumen del trabajo:

- Descripción de la infraestructura tecnológica implantada en la Administración de Justicia de Andalucía. Aspectos funcionales necesarios que se han tenido en cuenta para asegurar el éxito de la implantación.

Formato fichero:

- Word97

VENTAJAS DE LA APLICACIÓN DE LA FIRMA ELECTRÓNICA EN LOS PROCESOS JUDICIALES.

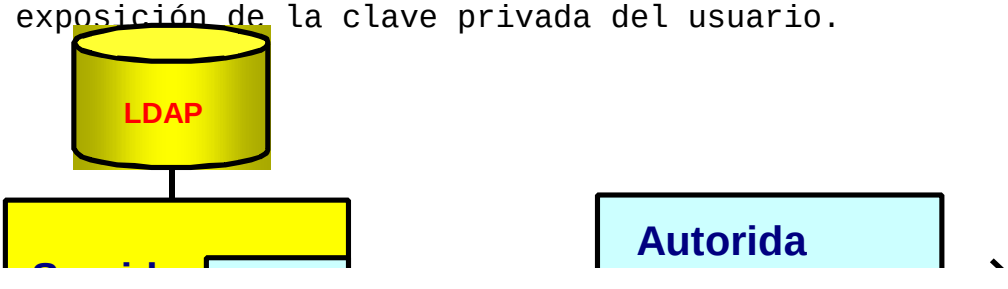
La Consejería de Justicia y Administración Pública de la Junta de Andalucía, lleva a cabo un proyecto para la incorporación de las funciones de FIRMA ELECTRÓNICA en las aplicaciones que soportan la ejecución de los procesos judiciales realizados dentro de la Comunidad Autónoma Andaluza.

Desde la transferencia de las competencias de Justicia a la Junta de Andalucía, hace aproximadamente tres años, dicha entidad puso en marcha el Plan Adriano, el cual centra su atención en todas aquellas actuaciones tendentes a la modernización de la Justicia en Andalucía, así como de sus infraestructuras. Ahora, mediante este nuevo proyecto, se pretende construir un sistema de seguridad que permita la ejecución de los trámites procesales, bajo unas condiciones que garantizan el máximo cumplimiento de la normativa existente tanto en materia de seguridad general como de firma electrónica en particular.

A continuación se describen las funciones y componentes que conforman el proyecto:

Se constituye una Autoridad de Certificación de índole interna para la Organización Judicial andaluza que incluye todos los componentes software y hardware necesarios para superar los requerimientos de seguridad fijados por las normativas existentes, tanto a nivel nacional como de la Unión Europea. En concreto, se contempla la implantación de un sistema de Infraestructura de Clave Pública que incorpora Autoridad de Certificación y de Registro para gestión de certificados, así como directorio LDAP y servidor Web para publicación de los certificados y listas de revocación. La Autoridad de Certificación incorpora un hardware criptográfico que garantiza la inaccesibilidad a su clave privada.

Los certificados y las claves correspondientes a los Jueces , Secretarios y Fiscales son generadas y almacenadas en tarjetas inteligentes criptográficas Bull TBC80 que aseguran la generación interna de las claves y realización de los algoritmos criptográficos. Con el objetivo de garantizar que las claves privadas de los usuarios nunca salen de la tarjeta criptográfica, se lleva a acabo una integración del software de Autoridad de Certificación (KeyOneCA de SafeLayer) con la estampadora de tarjetas. Esta integración permite un personalización total, tanto del plástico como de chip en una sola pasada, asegurando la firma del certificado por la CA sin exposición de la clave privada del usuario.

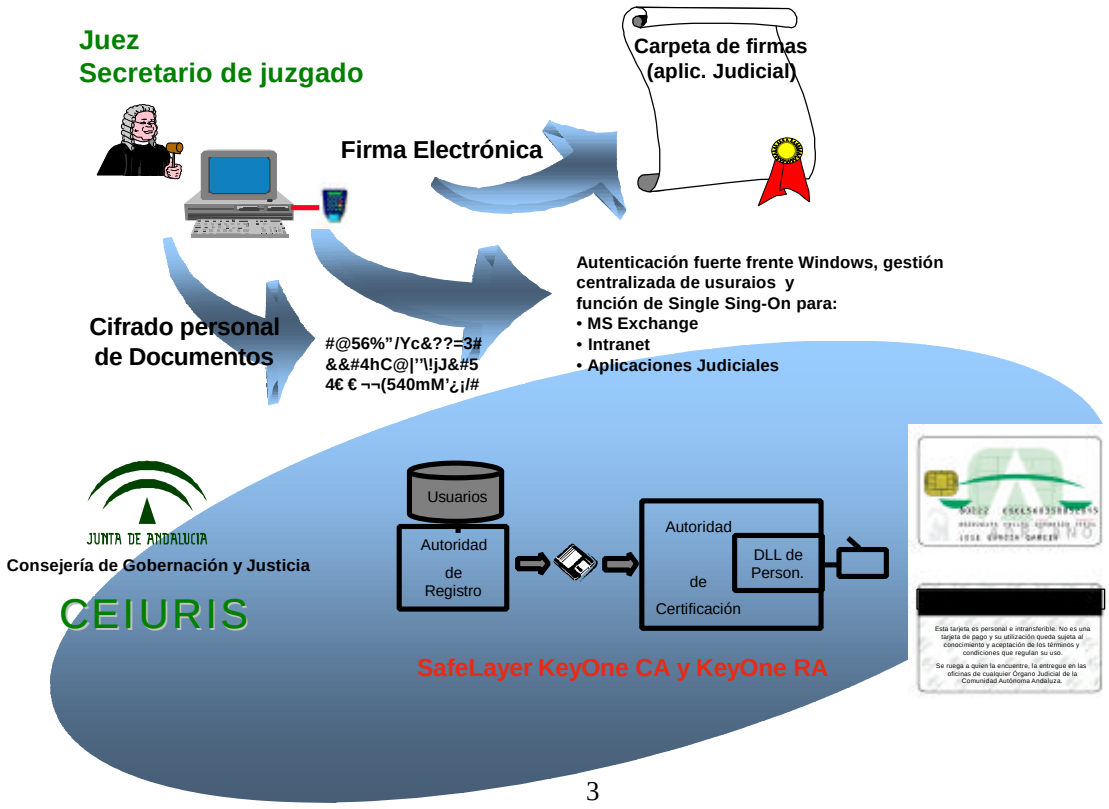


Se construyen las funciones criptográficas de firma electrónica, cifrado de documentos y verificación de firma y se incorporan a las aplicaciones usuales utilizadas en la realización de los trámites procesales.

La Consejería de Justicia y Administración Pública, lleva a cabo la incorporación de las funciones criptográficas en las aplicaciones destinadas a dar soporte a los trámites procesales realizados en:

- Juzgados de Instrucción
- Juzgados de 1ª Instancia
- Juzgados de lo Penal
- Audiencias Provinciales
- Juzgados de lo Contencioso Administrativo
- Salas del Tribunal Superior de Justicia de Andalucía

Como complemento necesario al proceso de incorporación de la firma electrónica, se lleva a cabo la securización del correo electrónico y de la Intranet Corporativa, mediante la utilización de la tarjeta criptográfica y certificado X.509.v3 para la autenticación, firma de mensajes y cifrado de las informaciones intercambiadas.



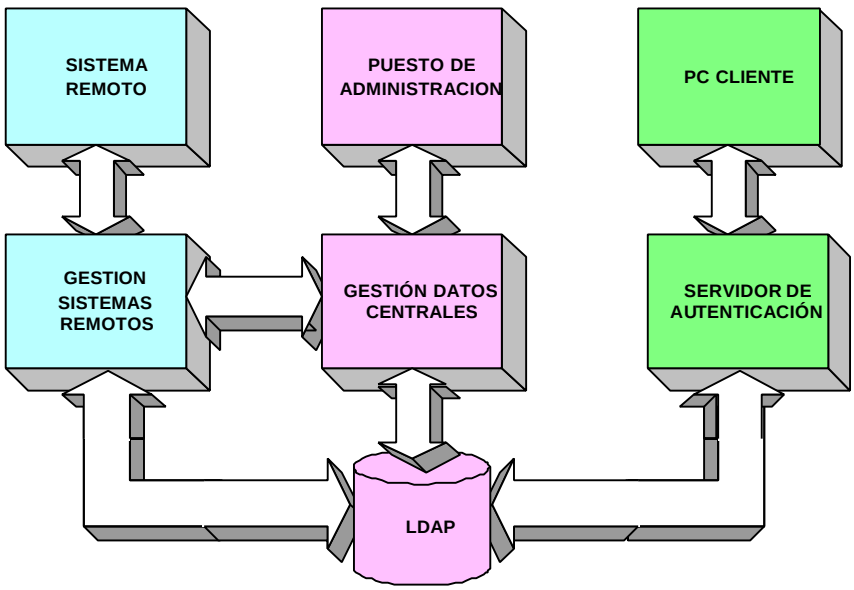
Finalmente, con el objetivo de construir un sistema dotado de la máxima seguridad, siempre mediante la utilización de las nuevas tecnologías basadas en tarjetas criptográfica y certificados, se implantan un conjunto de funciones de seguridad adicionales esenciales en un entorno altamente sensible como es el judicial:

- Autenticación reforzada para el control de acceso al puesto de trabajo mediante la utilización de la tarjeta criptográfica y el reconocimiento del certificado. Además, el usuario dispone de la función de autenticación única, de manera que, una vez autenticado en el arranque del puesto, accede a las aplicaciones sin necesidad de teclear ningún otro identificativo.

    - Gestión de usuarios y cuentas mediante su centralización en un directorio LDAP de la Organización.

    - Acceso protegido a servidores de grupo de trabajo mediante tarjeta inteligente y certificado

    - Construcción y gestión de una red privada virtual de 150 nodos (edificios donde se localizan los Órganos Jurisdiccionales), basada en la implantación de hardware criptográfico especializado que permite un ancho de banda de hasta 100 Mbits/seg.



ASPECTOS TÉCNICOS Y ORGANIZATIVAS DE LA IMPLANTACIÓN DE LA FIRMA DIGITAL EN ADRIANO.

- Se instala una Autoridad de Certificación (CA) en CEIURIS para la Administración de Justicia en Andalucía. La infraestructura de clave pública (PKI) implantada, sigue las más estrictas reglas de seguridad en la generación de la clave privada de la CA y su almacenamiento (se genera y almacena mediante un dispositivo Hardware, situada en una sala exclusiva de seguridad, a la que sólo se accede mediante tarjeta magnética y clave). Dicha sala se encuentra provista de alarma y sistema de extinción de incendios.

- La infraestructura de clave pública permite disponer a los usuarios de la Red Judicial de Andalucía, de 4 funcionalidades genéricas:

1. **Firma digital de documentos**. Mediante ella, se dota al sistema de los siguientes aspectos de seguridad:

   - **Autenticidad de Documentos**: un documento firmado permite identificar a su autor de forma segura y sencilla por el sistema.
   - **Integridad de documentos:** un documento firmado permite a su autor y a cualquier usuario del sistema detectar si un documento ha sido modificado después de haber sido firmado por su autor.
   - **No repudio:** los mecanismos de seguridad utilizados para la implantación de la firma digital hacen prácticamente imposible la falsificación de la firma digital, y por el mismo motivo, el que el autor de la firma niegue su autoría.

   El sistema contempla la posibilidad de la firma múltiple (un documento es firmado por más de una persona sucesivamente).

2. **Cifrado de documentos:** se trata de un cifrado personal de documentos, a diferencia del genérico que para las comunicaciones se implanta en Adriano (cifrado mediante cajas negras de cifrado, constituyéndose una auténtica Red Privada Virtual). Este cifrado personal dota al sistema de un nuevo aspecto de seguridad: **la confidencialidad**, en 2 sentidos:

   - **Confidencialidad de un documento para su autor:** el usuario cifra un documento usando su propia clave pública: sólo él puede descifrarlo, pues sólo él posee su clave privada, y por tanto sólo él tiene acceso al contenido del documento.
   - **Confidencialidad de un documento para un tercero:** y sólo para él. Un usuario cifrará un documento

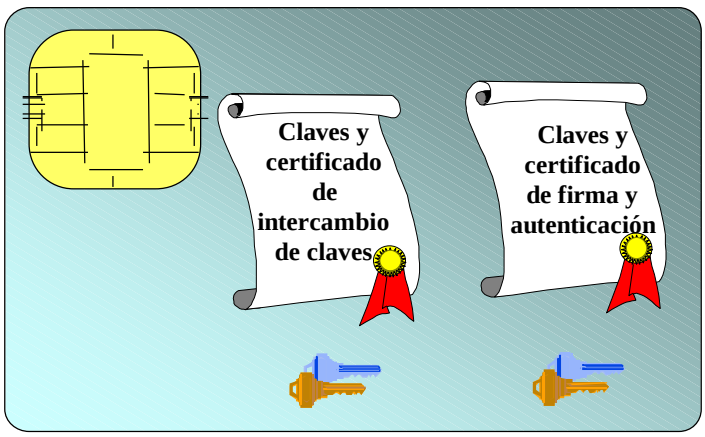
utilizando la clave pública del único usuario que desea tenga acceso al documento. Sólo este usuario, al ser el único que pose la clave privada correspondiente, tienen acceso al contenido del documento.

3. **Descifrado de documentos:** lo harán los usuarios mediante su clave privada.

4. **Reconocimiento de firma:** mientras que las 3 anteriores funcionalidades están disponibles sólo para los usuarios generadores de información sensible (Jueces, Secretarios Judiciales y Fiscales), esta cuarta funcionalidad lo está para cualquier usuario del sistema. Cualquier usuario puede reconocer quién es el autor (ó autores) de la firma digital de un documento y si un documento firmado ha sido modificado posteriormente a la firma. Por supuesto permite detectar la validez de la firma (es decir, si es una firma reconocida, si no ha sido revocado, etc.), e informa de ello al usuario que reconoce la firma. En cada reconocimiento de firma, desde las aplicaciones, se accede a un fichero generado por la CA y situado en uno de los Servidores de CEIURIS, que contiene la relación de los Certificados revocados (sin validez).

- Se generan **2 pares de claves pública-privada** en el sistema:

1. Par de claves para la firma digital de documentos.
2. Par de claves para el cifrado personal de documentos.



Las razones por las que se generan estos 2 pares de claves se explican más adelante.

- El soporte físico para las claves y certificados (clave pública firmada por la clave privada de la CA) es la

tarjeta inteligente criptográfica de última generación: permiten la generación de claves públicas-privadas dentro de la propia tarjeta inteligente. A la tarjeta sólo se puede acceder mediante un lector conociendo su PIN exclusivo. La actuación es distinta dependiendo de que se trate del par de clave para la firma ó para el cifrado.

1. En el caso de la **firma digital:** el par de claves se genera dentro de la propia tarjeta y **la clave privada jamás sale de la tarjeta. La clave privada no la conoce nadie, ni siquiera el propietario. Esto es una garantía más del no repudio.** La clave pública se extrae de la tarjeta, se genera el certificado correspondiente, se firma con la clave privada de la CA, y éste se vuelve a introducir en la tarjeta. Fuera permanece sólo la clave pública.

2. En el caso del **cifrado personal:** el par de claves se genera en el exterior de la tarjeta, introduciéndose después la clave privada y el certificado en la misma. En este caso de la clave privada de cifrado se conserva una copia fuera, en un dispositivo de alta seguridad. La razón de esto es impedir que un documento cifrado permanezca invisible incluso para su autor, si éste pierde la tarjeta inteligente, ó esta se inutiliza: siempre se podrá recurrir a la copia guardada en caso de necesidad.

- Tal y como se ha realizado la implantación de la firma digital en Adriano, cuando un documento se firma, se incluye: el documento firmado y el certificado del que firma. Ello permite a otro usuario, realizar el reconocimiento de la firma sin nada más que el documento firmado y el certificado en él incluido. Para asegurar que no se ha suplantado la identidad del firmante es para lo que se utiliza la clave pública de la CA. Esto es lo único que aporta el usuario que reconoce la firma: el certificado de la CA, que por otra parte, es algo público. La comprobación crítica del que reconoce la firma es realmente que el certificado del usuario firmante está firmado por la CA reconocida.

  En todos los clientes (en todos los Pc's de Adriano) se instala, para le reconocimiento de la firma, el certificado de la CA.

- Las **longitudes de las claves** públicas-privadas, son las siguientes:

  1. Las claves pública y privada de la CA: **2.048**
  2. Las clave pública y privada de usuarios, tanto de firma como de cifrado: 512 provisionalmente porque son las

que admite Windows a la fecha: Sin embargo, Adriano ya tiene previsto, en un plazo inferior a 1 año (cuando lo permita Windows) sustituirlas por claves superiores (**1.024**).

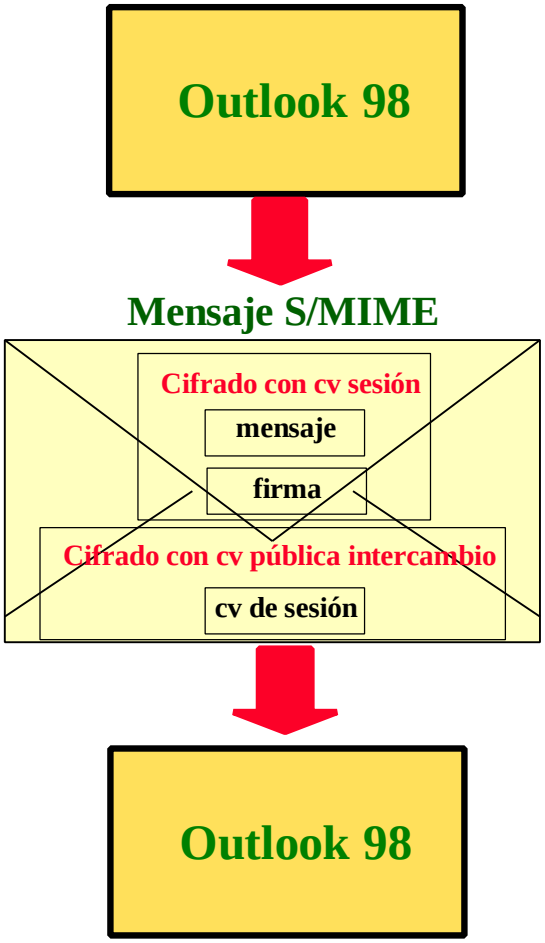
- La implantación de la **firma digital** en la Red Judicial de Andalucía ha sido concebida como una herramienta que dota al sistema de aspectos muy importantes de seguridad adicionales. Es importante destacar lo siguiente:

1. No se pretende la sustitución de la firma manuscrita, ni la supresión del papel. Sin embargo, sienta las bases para que algún día, con el soporte legal y normativo necesario, se realice. Dicho de forma sintética, el sistema estará preparado para cuando ese día llegue.
2. El sistema no obliga al uso de las funcionalidades de seguridad que permite la implantación de la firma. Es una herramienta al servicio del usuario autorizado a su uso, pero por supuesto se permite que no llegue a usarse nunca por alguno, si así lo decidiera.
3. Se ha diseñado de forma que su uso sea simple y no ralentice en ningún caso el sistema. Inicialmente, el que un documento esté firmado o no, no detiene la tramitación del asunto al que pertenece (aunque se contempla que algún día pueda llegar a ser así, en los puntos de tramitación que se decidiera).

- Adriano pretende implantar la firma en las siguientes aplicaciones:

1. **Aplicación de Gestión Procesal:** mediante un módulo especial de la aplicación, que nosotros llamamos **Carpeta de firma,** se permite al usuario de tarjeta inteligente acceder a todos los documentos generados por la tramitación del asunto que aún no han sido firmados y firmarlos. La firma se puede realizar de todos los documentos seleccionados, por lotes, ó bien uno a uno, visualizándolos previamente.
   La firma desde la carpeta de firma ha sido ideada para que sea usada fundamentalmente por los Secretarios Judiciales.
   Hay un aspecto importante en cuanto al reconocimiento de la firma: el usuario lo hace utilizando el editor de texto integrado en la propia aplicación (es una función del propio editor). La peculiaridad es que el editor es capaz de reconocer el documento que ha sido firmado, y el que lo está, lo abre en modo de **sólo lectura**, garantizando que no sea modificado por el usuario de tramitación después de que haya sido firmado.
   El reconocimiento de la firma desde la aplicación ha sido diseñado para cualquier usuario de la misma.

2. **Aplicación de Correo Electrónico:** la Red Judicial de Andalucía dispone de su dominio de correo electrónico. Los usuarios generadores de información sensible dispondrán de su propia cuenta de correo corporativo. El cliente de correo electrónico corporativo será Outllook (actualmente Outlook Express). La utilización de la firma desde este cliente es sencilla. Consiste en una casilla de verificación tanto para la firma como para el cifrado. Tiene, además, los siguientes aspectos interesantes:
   - Un mensaje puede ser firmado, y además, cifrado.
   - Cuando un mensaje es firmado y/o cifrado, se firma y/o cifra todo el mensaje incluyendo los documentos adjuntos.
   - Es el correo dónde el sistema incorpora la firma de documento para un tercero: en este momento se accede al directorio LDAP, ubicado en un servidor de CEIURIS, para conseguir el certificado del usuario al que se desea enviar el mensaje cifrado.



Esta aplicación estará a disposición de cualquiera de los funcionarios de la Administración de Justicia de Andalucía generadores de información sensible (Jueces, Secretarios Judiciales y Fiscales).

3. **Aplicación específica de firma:** esta aplicación permite realizar cualquiera de las funcionalidades descritas (firma, reconocimiento de firma, cifrado, descifrado) sobre cualquier tipo de documento. Permitirá además el **borrado irrecuperable, solicitando confirmación,** de cualquier fichero del sistema. En la acción de cifrar cualquier documento se pedirá la confirmación para borrar de forma segura (borrado irrecuperable) el documento original.

   Esta aplicación estará a disposición de cualquiera de los funcionarios de la Administración de Justicia de Andalucía generadores de información sensible (Jueces, Secretarios Judiciales y Fiscales).

- Algunos aspectos añadidos al uso de tarjeta inteligente:
  La Junta de Andalucía ha añadido la siguiente funcionalidad en el uso de la tarjeta inteligente: para Pc's de Jueces, Secretarios Judiciales y Fiscales, cuando el PC arranca, pide que se inserte la tarjeta inteligente y que se teclee el PIN. La pantalla inicialmente permite cancelar, y entonces pide la contraseña del usuario. Aunque, si así lo decidiera algún usuario, podría suprimirse la posibilidad de cancelar. De esta manera se puede llegar a impedir que se acceda a un Pc de usuario si no tiene la tarjeta ó no conoce el PIN. Una vez tecleado el PIN adecuado, el usuario se conecta tanto a red local, como al correo electrónico, como a la aplicación. El PIN se volverá a pedir al usuario cada vez que este realice una función de seguridad (firma, cifrado, arranque de la aplicación de gestión procesal, de la aplicación de correo, etc.), siempre y cuando el tiempo transcurrido desde la última vez que se solicitó el PIN fuera superior a 1 minuto (este es un parámetro modificable).

- La aplicación ha establecido los siguientes protocolos para la entrega, revocación y corrección de certificados a los usuarios de la Red Judicial de Andalucía.

1. **Entrega inicial masiva**: Se genera de forma masiva las claves privadas y los certificados de usuarios, y las tarjetas que lo soportan.
   Se entrega personalmente a cada usuario su tarjeta inteligente, personalizada. La tarjeta lleva el nombre del usuario propietario y una codificación que la identifica. Todos los usuarios dispondrán, en el escritorio de su Pc, de una aplicación que permite modificar el PIN de la tarjeta. Se generará un PIN inicial común para todos que debe ser modificado inmediatamente por el usuario.

2. El control para la conexión de un usuario a la aplicación judicial, está en manos del Secretario Judicial, que es el

que puede dar de alta a usuarios en la aplicación. Un usuario de tarjeta inteligente podrá tener acceso a los datos de su juzgado cuando el Secretario Judicial lo decida. Cuando un usuario de tarjeta inteligente realiza una sustitución en otro juzgado, podrá usar su misma tarjeta personal que usaba en el otro juzgado, y el acceso lo decidirá el Secretario Judicial. Sólo en el caso de que este mecanismo sea inviable, se actuaría desde CEIURIS. Del mismo modo, un Secretario Judicial podrá dar de baja (deberá darse de baja a sí mismo, si fuera el caso) en un juzgado al usuario (por ejemplo, Juez) sustituido. Esto sigue siendo válido cuando la sustitución sea temporal.

3. Cuando un Juez, Secretario Judicial, ó fiscal, se incorpora por primera vez como usuario de tarjeta inteligente de la Red Judicial de Andalucía, se ha ideado el siguiente protocolo:

    1. Otro usuario de tarjeta inteligente ya existente en el sistema, avala la incorporación del nuevo usuario. Para ello firmará un documento electrónico (modelo preestablecido) convenientemente completado con los datos necesarios para la elaboración del certificado del usuario, y lo enviará mediante correo electrónico firmado y cifrado a CEIURIS.
    2. En CEIURIS, una vez reconocida la firma del avalista, se generará el certificado y la tarjeta inteligente del nuevo usuario.
    3. Se hará llegar, desde CEIURIS y de forma segura, la tarjeta y el PIN inicial de la tarjeta.

    De esta manera, son las propias sedes judiciales las que de alguna manera actúan como autoridades de registro.

    Las pérdidas de tarjetas, olvidos de PIN, etc. se comunicará telefónicamente a CEIURIS, al área de atención de usuarios, que dará de baja la tarjeta y generará una nueva para ese usuario, haciéndosela llegar por el procedimiento seguro anterior.