1 Resumen

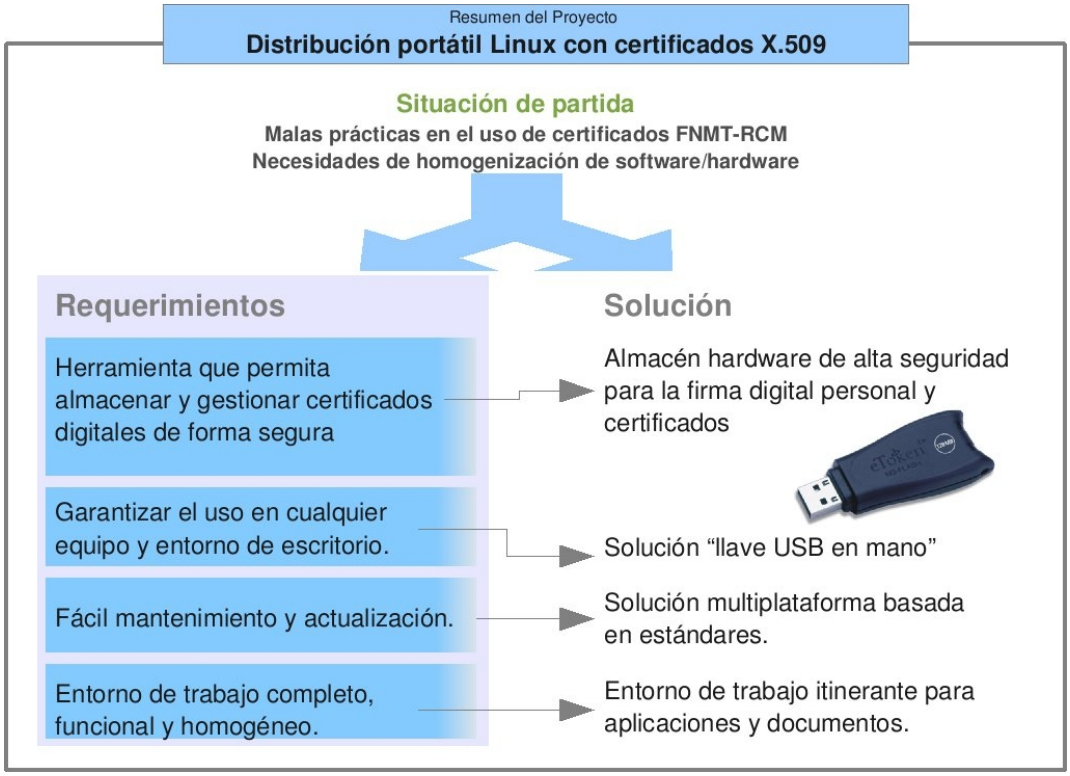
El proyecto *Distribución portátil Linux con certificados X.509* es una iniciativa orientada a la implantación efectiva del uso de certificados digitales y de la propia plataforma de administración electrónica de la Diputación Provincial de Teruel. Los usuarios a los que se ha destinado la solución son los usuarios internos de la Diputación.

La solución consiste en un "almacén de certificados", al mismo tiempo que una distribución Linux a medida con un conjunto de aplicaciones de uso común por defecto. Este almacén de certificados se encuentra protegido físicamente en un dispositivo tipo USB token, que a su vez dispone de memoria en la que alojar software y documentos.

La funcionalidad más relevante que aporta la solución, es que permite al usuario el acceso desde el navegador web a cualquier sitio, identificándose mediante los certificados correspondientes, gracias a la integración de certificados x 509 personales para cada uno de los dispositivos.

Adicionalmente las aplicaciones están integradas por defecto con el almacén de certificados, por lo que no es necesario configurarlas. Otro de los puntos fuertes es que el almacén de certificados es hardware, con lo cual tiene un alto nivel de protección frente a accesos no autorizados.

El proyecto se encuentra actualmente en fase de despliegue en paralelo con la progresiva implantación de la plataforma de administración electrónica de la Diputación Provincial de Teruel. El alcance del proyecto es servir a más de 200 Ayuntamientos y 10 comarcas con las que han firmado el Convenio de Teleadministración y que forman parte del mapa de usuarios internos de la Diputación Provincial de Teruel.



2 Justificación del proyecto

Marco de Actuación

El Proyecto **Distribución portátil Linux con certificados X.509** se enmarca dentro del conjunto de actuaciones en curso de la Diputación Provincial de Teruel destinadas a implantar las medidas necesarias para hacer efectivo el cumplimiento de lo especificado dentro de la **Ley 11/2007**, de 22 de junio, Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

En este contexto, la Diputación Provincial de Teruel ha iniciado un proceso de modernización administrativa, dirigido a la propia Diputación y al conjunto de Entidades Locales de la provincia, que tiene dos objetivos fundamentales y complementarios:

- Proveer las herramientas y sistemas informáticos que faciliten la automatización y optimización de la gestión administrativa, de modo que se reduzcan los plazos de tramitación y se haga un uso más eficiente de los recursos disponibles.
- Favorecer los mecanismos necesarios para la implantación de servicios públicos electrónicos, cumpliendo de este modo lo establecido en la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Motivación

Al igual que en la mayoría de las administraciones públicas, el entorno tecnológico para el acceso a la administración electrónica en la Diputación Provincial de Teruel incluye la utilización de los certificados de la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (en adelante FNMT-RCM).

En cuanto al equipamiento necesario, el soporte utilizado para incrementar la seguridad del sistema de certificación son las **tarjetas criptográficas** y los correspondientes **dispositivos lectores de tarjeta** incorporados en el teclado.

En este escenario, la **principal motivación del proyecto Distribución portátil Linux con certificados X.509** fue la **solución de malas prácticas en el uso de los certificados** de la FNMT-RCM por parte de los usuarios internos de la Diputación Provincial de Teruel y que comprometían la efectiva implantación de la plataforma de administración electrónica.

Entre las deficiencias más relevantes se observaron las siguientes:

- **Uso compartido no autorizado de claves y contraseñas**
- **Almacenamiento de certificados y contraseñas sin garantías de seguridad**

La preocupación de la Diputación de Teruel con relación a estas situaciones les llevó a plantearse el origen de esta situación y cómo solucionarla. En este sentido, algunos de los comportamientos observados incluían por ejemplo faltas relacionadas con el principio de identidad asociado intrínsecamente al uso de certificados, ya que los certificados eran compartidos por los usuarios, por otro lado, también se observó de forma recurrente el almacenamiento de los certificados en los navegadores web o en el escritorio, lo que supone una alta vulnerabilidad de seguridad.

Cómo resultado, se determinó que además de posibles fallos humanos o de necesidades de formación, existen al menos dos factores que podrían explicar dichos comportamientos ya que obligaban a los usuarios a trabajar en equipos que no han sido configurados con su información personal. Se determinó que los factores que podrían controlarse de forma inmediata eran:

1. La tarjeta criptográfica no puede ser utilizada en todos los equipos, por lo que habría

que buscar una solución que fuera compatible con el equipamiento disponible.

2. Los puestos de trabajo no tienen un escritorio homogéneo y/o no tienen instaladas las aplicaciones específicas para interactuar con la plataforma de administración electrónica de la Diputación de Teruel, por que habría que encontrar una solución que incorporara las aplicaciones necesarias.

3 Objetivos del proyecto

Con la finalidad de subsanar los problemas detectados en el uso de certificados digitales por parte de su personal interno, la Diputación Provincial de Teruel se planteó los siguientes objetivos:

- Dotar a los funcionarios de una herramienta que les permitiera **almacenar y gestionar los certificados de forma segura** para interactuar con la plataforma de administración electrónica.
- Ofrecer a los usuarios internos un **entorno de trabajo completo, funcional y homogéneo** para el acceso a la plataforma de administración electrónica.
- Garantizar el uso de la herramienta seleccionada **en cualquier equipo y entorno de escritorio.**
- **Facilitar el mantenimiento y actualización de aplicaciones en uso.**

4 Solución Técnica

Sobre los requisitos planteados por la Diputación Provincial de Teruel, el equipo de Warp Networks diseñó una solución basada en los siguientes elementos:

- Solución “llave USB en mano”
- Almacén hardware de alta seguridad para la firma digital personal.
- Entorno de trabajo itinerante para aplicaciones y documentos.
- Solución multiplataforma basada en estándares.
- Herramientas operativas.

Solución “llave USB en mano”

El software resultante incluye todo lo necesario para trabajar en una sencilla llave USB. Tanto el almacén hardware como la memoria y el propio entorno de trabajo están incluidos en este dispositivo, y son accesibles a través de sencillos menús gráficos.

Almacén hardware de alta seguridad para la firma digital personal

Cada funcionario dispone de una llave en cuyo interior se halla integrado un componente electrónico que implementa un almacén hardware de alta seguridad para su firma digital personal.

Dicho almacén está protegido mediante una contraseña y contra accesos físicos, de manera que la pérdida del mismo no implica un compromiso de las firmas digitales, en contraste a otras soluciones como portar las claves en un simple fichero de texto.

Tras evaluar diferentes soluciones, sometiéndolas a diversas pruebas de laboratorio referentes

a su operativa, compatibilidad y estabilidad, se optó por el token Aladdin eToken NGFlash.

El eToken NGFlash es una **tarjeta inteligente USB sin necesidad de lector.** Este dispositivo de bajo coste permite la autenticación fuerte de doble factor. La seguridad del eToken se basa en el algoritmo RSA integrado de 1024 y de 2048 bits, con lo que permite una integración perfecta con cualquier arquitectura PKI y otras arquitecturas de seguridad. Adicionalmente cuenta con una memoria flash encriptada, para un almacenamiento seguro de datos móviles.

Las características principales del eToken NGFlash son:

- Soporte de certificados X.509.
- Interfaces API & normas admitidas: PKCS#11 v2.01, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE
- Homologaciones de seguridad: Common Criteria EAL4/EAL4+ (smart card chip) Pendiente: FIPS 140-2 (complete device).
- Compatibilidad con homologaciones ISO: Compatibilidad con especificaciones ISO 7816-1 a 4.
- Hasta 4Gb de memoria flash: Lo que permite contar con espacio suficiente para almacenar tanto aplicaciones como documentos.
- Alta resistencia a un uso continuado: garantía de al menos 10 años en retención de datos en memoria de tarjeta inteligente y 500.000 reescrituras de celdas de memoria.

Este almacén está integrado con los procesos y aplicaciones de firma digital implantados en la Diputación Provincial de Teruel, incluyendo el soporte de firmas, la autoridad de certificación, o los procedimientos de solicitud, obtención, caducidad, revocación, etcétera. En este caso, todos los certificados, para ser tales y evitar su alteración o falsificación, deben estar respaldados por el certificado raíz de la Fábrica Nacional de Moneda y Timbre (FNMT-RCM).

Además, el **software integrado en el dispositivo permite la gestión y acceso a los certificados, tanto los personales de los usuarios como los de las autoridades de certificación incluidas**, por medio de herramientas y documentación.

Entorno de trabajo itinerante para aplicaciones y documentos

El entorno de trabajo está compuesto por las aplicaciones y documentos que se utilizan para realizar el trabajo diario por parte de los funcionarios.

En el caso de las aplicaciones, después de realizar un análisis se determinó que estas eran principalmente:

- Aplicaciones de la Diputación Provincial de Teruel.
- Navegador web (con soporte de WebSigner para el acceso a la Plataforma de Adminsitración Electrónica) y cliente de correo electrónico.
- Procesador de textos, hoja de cálculo y software para presentaciones.
- Software de gestión del almacén de firma digital.
- Enlaces a recursos y webs de utilidad.

El otro elemento principal son los documentos sobre los que se está trabajando, incluyendo por ejemplo las memorias, tramitaciones, etcétera, o los diferentes proyectos que deben gestionarse en el día a día.

La solución desarrollada **permite el acceso a las aplicaciones desde cualquier tipo de**

equipo de sobremesa o portátil, conservando el estado del entorno de trabajo así como la configuración del mismo. De esta manera, la colocación de los iconos en pantalla, o los tipos de letra usados en los textos, "viajan" con el usuario.

Dichas **aplicaciones están preconfiguradas para integrarse con el almacén hardware**. De esta forma, el navegador web usará la identidad protegida en el mismo para presentarse ante el navegador web, o el procesador de textos firma digitalmente los documentos con la identidad del funcionario, sin necesidad de procesos de configuración tediosos o difíciles de comprender.

Todo el entorno de trabajo de los funcionarios se basa en una distribución de software libre Ubuntu, por lo que **el desarrollo comparte la misma base empleada por las Administraciones Públicas de Extremadura, Andalucía, Madrid, Valencia y Castilla La Mancha**. La primera solución utilizaba la versión 8.04, y la última actualización la 9.10. Además de asegurar la viabilidad técnica de la solución, y permitir una personalización de elementos como la identidad corporativa, idioma, aplicaciones, etc..., esto **minimiza los costes asociados a la adquisición y gestión de licencias**.

El trabajo de personalización incluyó tanto la adaptación del interfaz de usuario a las necesidades de los funcionarios, facilitando tareas como el acceso a sitios recurrentes mediante enlaces, como la propia modificación del dispositivo a bajo nivel, trabajando con el equipo de ingenieros de Aladdin en Israel y Alemania. En todo momento se gozó de un soporte técnico irreprochable, que permitió consolidar todos los aspectos de la solución.

Gracias al empleo simultáneo de tres sistemas de ficheros, comprimidos, en RAM y de apilamiento, se incluyen más de 2 GB de aplicaciones comprimidos en apenas 700MB, que son accesibles al vuelo, en modo "live". Esta infraestructura es de vital importancia, ya que el tamaño disponible sin comprimir en la memoria RAM es de 1 GB.

Para usar el sistema, simplemente debe introducirse la llave en un slot USB, y proceder a continuación a arrancar el computador. Gracias a las modificaciones realizadas en diversos elementos como el gestor de arranque, las tablas de particionado y los sistemas de ficheros, el usuario simplemente tendrá que introducir una contraseña para poder usar todas las aplicaciones incluidas.

Solución multiplataforma basada en estándares

El sistema es multiplataforma, **permitiendo su ejecución en cualquier tipo de PC o portátil dotado de una ranura USB**, independientemente del sistema operativo (Windows/ MAC / Linux) o aplicación instalado en el equipo.

Además, todas las aplicaciones incluidas trabajan con estándares abiertos y libres de patentes y del pago de regalías, como son:

- Especificaciones del World Wide Web Consortium (W3C)
- Estándar ISO/IEC 26300:2006, Open Document Format (ODF)
- Estándar ISO 19005-1:2005, Portable Document Format (PDF/A)

Herramientas operativas

Con el fin de facilitar la gestión de la solución por parte del personal informático de la Diputación Provincial de Teruel, el software viene acompañado de una serie de herramientas, que permiten por ejemplo:

- Personalizar de forma simultánea uno o varios dispositivos con el software y la configuración apropiada.

- Devolver el sistema instalado en un dispositivo a su configuración original, borrando todas las modificaciones y datos personales introducidos por los usuarios.

Además, se dispone de paquetes de la distribución para todos los datos susceptibles de cambiarse en el tiempo, como los marcadores, de manera que, desde un repositorio interno es posible modificar la identidad, los enlaces, etc... de una manera transparente al usuario final del dispositivo.

5 Aplicaciones futuras

La solución desarrollada ha abierto el camino a la inclusión de nuevos servicios integrados, que incrementen el valor aportado a sus usuarios. Entre los elementos presentes en las próximas versiones están:

- **Aplicaciones portables MS Windows**

  Como complemento al entorno de trabajo preconfigurado, se añadirán aplicaciones portables para Windows, por ejemplo navegadores de texto, clientes de correo electrónico o suites ofimáticas, integradas con el almacén del claves hardware de forma automática. Se persigue poder arrancar dichas aplicaciones desde el token sin alterar el equipo desde el que se lanza, para aquellos usuarios que posean una copia legítima de Microsoft Windows.

- **Integración VPN**

  Dentro del área de conectividad, se prevé la integración de una serie de soluciones para redes privadas virtuales (VPN), de modo que la autenticación se realice también de forma transparente a través del propio almacén de claves hardware, y las aplicaciones vengan preconfiguradas para evitar que los funcionarios deban recurrir a los servicios de soporte técnico para ello.

- **Integración aplicaciones de terceros**

  Dado el interés mostrado por algunos de los clientes en soportar aplicaciones de terceros, se prevé la inclusión de algunas de ellas en un futuro cercano. Entre las aplicaciones de mayor entidad sobre las que se ha realizado un estudio técnico, se incluye la suite Lotus Notes de IBM, que cuenta con una versión nativa para Ubuntu Linux.

- **Firma digital directa**

  Con el objetivo de facilitar al máximo el empleo de la firma digital, se ha diseñado un sistema que permite ejecutarla de forma natural, usando un único click o un sencillo interfaz de arrastrar y soltar, usando de forma transparente el almacén hardware presente en el dispositivo.

- **Seguridad biométrica**

  La evolución del hardware actual incluye algunos modelos con un lector de huellas digitales, que ofrecen un nivel adicional de seguridad. De este modo, cada token estaría protegido no solo por una contraseña, sino también por una identificación biométrica, pero manteniendo el mismo nivel de sencillez de uso del que goza actualmente.

- **Clave única en el arranque**

  Como mejora de usabilidad, se plantea la integración con el gestor de carga. De esta manera, al arranque del sistema, usando la contraseña que desbloquee la firma digital, la solución arrancaría completamente, entrando en sesión de manera directa, evitando pedir contraseñas al usuario durante el resto de la sesión.

- **Cifrado multiplataforma del sistema de ficheros**

  El dispositivo actual permite el cifrado de los datos almacenados en la memoria, pero no puede hacerse de forma que resulte accesible desde varios sistemas operativos. Mediante el empleo de soluciones de cifrado multiplataforma, se persigue mejorar ese aspecto.

Las consideraciones anteriores y nuevos escenarios de uso constituyen una invitación a seguir trabajando en estas líneas de desarrollo, en cualquier Administración con problemáticas similares a las que planteaba la Diputación Provincial de Teruel al inicio del proyecto y que sin duda podrían ser detectadas en la medida en que se siga avanzando en proyectos internos relacionados con la implantación definitiva de la administración electrónica.

6 Datos de Contacto

- **Proyecto**
  - Distribución portátil Linux con certificados X.509
- **Entidad responsable del proyecto**
  - Servicio de Informática de la Diputación Provincial de Teruel.
- **Empresa desarrolladora:**
  - Warp Networks S.L
- **Autor:**
  - Ricardo Muñoz Fernández – Líder Técnico en Warp Networks (rmunoz@warp.es)
  - Calle Don Jaime I, 33 – 3ro derecha- 50003, Zaragoza. España. Tel.976 392 644 – Fax. 976 290 004. http://warp.es/