



# TrustedX: La custodia de documentos firmados

En este artículo se exponen las pautas estratégicas que ofrece la plataforma de firma electrónica TrustedX en materia de archivado y mantenimiento de firmas electrónicas a lo largo del tiempo.

Se entiende por archivado como el almacenamiento en repositorios de documentos y firmas electrónicas, junto con sus correspondientes metadatos, durante periodos de tiempo de larga duración. La custodia implica garantizar la preservación de las firmas, de forma que éstas no pierdan su valor probatorio después de durante un determinado período de tiempo.

El módulo de custodia de la plataforma TrustedX implementa las interacciones requeridas con repositorios de documentos para el archivado de documentos y firmas, así como, la gestión de los metadatos de firma. La preservación de las firmas se realiza según las recomendaciones de los estándares \*AdES de ETSI.

En cuanto al soporte de repositorios, TrustedX ofrece una arquitectura flexible permitiendo la adopción de diferentes estrategias de implementación. El archivado se puede implementar en una base de datos externa gestionada por la propia plataforma, apoyarse en sistemas de Fixed Content Storage y/o integrarse en gestores de contenidos DMS/ECM mediante el desarrollo de un plugin.

## Preservación de las firmas y movilidad

El proceso de verificación de firmas requiere la comprobación de la integridad del documento y recabar un conjunto de evidencias que permitan probar la validez de los certificados digitales en el momento de la firma, es decir que no se hubiesen revocado. Para que el proceso pueda realizarse después de que los certificados digitales hayan expirado, se requiere el archivado y el mantenimiento de dichas evidencias.

La información sobre el estado de los certificados se obtiene de forma online, mediante una conexión con el prestador de servicios de certificación (PSC) que emite los mismos. Además, esta información deberá protegerse criptográficamente, para asegurar la integridad de la firma a lo largo del tiempo.

La pérdida de información probatoria está relacionada con el paso del tiempo (las evidencias que en su día eran válidas dejan de serlo a partir de un momento determinado), pero también podría ser inherente a la movilidad del propio documento firmado (en implementaciones que emplean un depósito específico de evidencias al margen de las firmas] éstas sólo son válidas en el contexto del propio sistema de archivo).

La resolución del problema de la preservación de las firmas se detalló en la RFC 3126/5126 de IETF (Internet Engineering Task Force). Actualmente, las recomendaciones CADES, XAdES ó PAdES de ETSI (European Telecommunications Standards Institute), que soporta TrustedX, adoptan la propuesta inicial de IETF y definen los formatos de firma longevos, estableciendo cómo preservar las evidencias a lo largo del tiempo.

La estandarización y la orientación al documento son características esenciales que aportan dichas recomendaciones de ETSI. Es decir, las evidencias que aportan el valor probatorio se mantendrán en las propias firmas indistintamente de los repositorios en donde se archiven. Esta aproximación desacopla perfectamente el documento de los repositorios, posibilitando la verificación de firmas con herramientas de terceros, o simplemente permitiendo la migración de los documentos a otros sistemas sin perder valor probatorio.

### **Repositorios de documentos con firma electrónica**

Un aspecto inherente del archivado de los documentos firmados electrónicamente son las funciones relacionadas con la organización y gestión de éstos, sus propiedades o metadatos, flujos de trabajo asociados, conversión de contenidos y formatos, y en especial aquellos aspectos relacionados con la búsqueda de la información. Otras necesidades de archivado pueden ser las funciones de retención e integridad garantizada del contenido a largo plazo que ofrecen algunos sistemas de Storage.

Por poner un ejemplo, los gestores de contenidos proporcionan una experiencia de gestión documental especializada, aportando una consola de administración gráfica y un conjunto de herramientas de gestión que estos sistemas aportan de forma nativa. La posibilidad de integrar la plataforma de firma TrustedX a un sistema corporativo existente posibilita el uso de estos recursos en lugar de introducir los de un repositorio específico para tal efecto, lo que supone un ahorro de costes de formación y de costes de mantenimiento, además de la automatización de la gestión de las firmas.

Esta facilidad es algo que proveen de forma estándar los sistemas de gestión de contenidos DMS/ECM o Storage, por lo que se trata de componentes asociados a muchos escenarios habituales del sistema de custodia documentos. Pero, en estos escenarios, se trata de funcionalidades de difícil implantación si se utiliza para este fin otro tipo de repositorios, tal como las bases de datos.

Las funciones que implementa TrustedX, son las de archivado (envío de documentos para su custodia), verificación de estado (comprobación de estado de uno o más documentos), extracción de documentos (obtención de documentos firmados, en cuyo caso será posible su verificación por terceros), borrado (eliminación de documentos

firmados) y verificación (comprobación de las firmas de los documentos). Estas funciones son comunes indistintamente del tipo de repositorio que se use, pudiendo ser:

- Gestores de contenidos. TrustedX dispone de mecanismos de integración para poder usar un gestor de contenidos corporativo. En este caso, se requiere el desarrollo de un conector específico para la búsqueda de documentos, así como de un mecanismo de acceso a los mismos basado en clientes ligeros como HTTP/WebDAV.
- Base de datos externa. Esta opción, prevista para futuras versiones de TrustedX, soporta el archivado en bases de datos de Oracle. TrustedX se encarga de almacenar y mantener los documentos firmados base de datos, así como los metadatos asociados a la firmas.
- Sistemas de archivado<sup>1</sup>. Permite usar la infraestructura de Storage corporativa para el archivado de documentos mediante conectores. Soporta los sistemas de Storage de Centera de EMC.

En cuanto a los estándares técnicos de conexión a repositorios que ofrece TrustedX, pueden ser JDBC para BBDD (Oracle) o accesibilidad por medio de protocolos como HTTP/WebDAV (e.g. Alfresco o Documentum). En cuanto al soporte de sistemas de tipo Fixed Content Storage, tales como EMC Centera, se proporcionan conectores para las API de estos dispositivos. En todos los casos, TrustedX permite configurar políticas del servicio de manera que, con cada una de ellas, el archivado se realice en un repositorio diferente y/o con propiedades distintas.

---

<sup>1</sup> Opción disponible exclusivamente a través de algunos partners de Safelayer. Consultar para más información.