

El nuevo BOE Electrónico



David Guerrero <david@boe.es>
Boletín Oficial del Estado
Ministerio de la Presidencia
Septiembre 2008

PreparaTIC XVII
Madrid

Agenda

- LAECSP
- Real Decreto 181/2008 de ordenación del BOE
- Accesibilidad
- Firma Electrónica
- Impacto en Sistemas y Comunicaciones
- Impacto en el resto del Organismo

- DEMO ???

LAECSP (Ley de acceso electrónico de los ciudadanos a los Servicios Públicos)

Artículo 11. Publicaciones electrónicas de Boletines Oficiales.

- 1. La **publicación de los diarios o boletines oficiales en las sedes electrónicas** de la Administración, Órgano o Entidad competente tendrá, en las condiciones y garantías que cada Administración Pública determine, **los mismos efectos que los atribuidos a su edición impresa**
- 2. La **publicación del «Boletín Oficial del Estado» en la sede electrónica del organismo** competente **tendrá carácter oficial y auténtico** en las condiciones y con las garantías que se determinen reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables.

REAL DECRETO 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado»

- Se definen aspectos generales como:
 - Entrada en vigor: **1 de enero de 2009**
 - Además de la legalidad otorgada por la LAESCP a la edición electrónica, se asimila dicha legalidad a una edición impresa, derivada de la primera
 - **Edición impresa limitada** (menos de 10 ejemplares) y con características de perdurabilidad
 - Se define el formato:
 - Mono-disposición
 - Mono-columna
 - Código de verificación

REAL DECRETO 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado»

- Sobre la **edición electrónica**:
 - Se publicará en la **sede electrónica** del BOE, que se dotará de las medidas de seguridad que garanticen la **autenticidad** e **integridad** de los contenidos del diario oficial, así como el **acceso permanente** al mismo
 - Accesible en la sede electrónica en la fecha que figure en la cabecera del ejemplar diario, salvo que ello resulte imposible por **circunstancias extraordinarias de carácter técnico**
 - En este último caso, la edición impresa asegura la publicación

REAL DECRETO 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado»

- Sobre la **edición electrónica**:
 - Deberá incorporar **firma electrónica avanzada** como garantía de la autenticidad, integridad e inalterabilidad de su contenido.
 - Los **ciudadanos podrán verificar** el cumplimiento de estas exigencias **mediante aplicaciones estándar** o, en su caso, **mediante las herramientas informáticas que proporcione la sede electrónica de la Agencia Estatal Boletín Oficial del Estado**

REAL DECRETO 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado»

- Sobre la **edición electrónica**:
 - Respetará los principios de **accesibilidad** y **usabilidad**, utilizará **estándares abiertos** y en su caso aquellos otros que sean de uso generalizado por los ciudadanos
 - Corresponde al BOE **custodiar** y **conservar** la edición electrónica del diario oficial del Estado
 - Corresponde al BOE velar por la **permanente adaptación al progreso tecnológico**

Accesibilidad

- Se velará por la accesibilidad de:
 - La **sede electrónica** (página web)
 - Desaparición de la versión gráfica/texto (versión única basada en CSS)
 - Nuevo diseño con criterios AA (WAI)
 - El propio **Diario Oficial** publicado en PDF
 - Elección del formato PDF/A (archivo a largo plazo)
- Estrecha colaboración con el **Centro de Referencia en Accesibilidad y Estándares Web (INTECO)**

Accesibilidad

- PDF/A (ISO-19005-1)
 - Versión “reducida” del estandar PDF 1.4
 - **PDF/A-1b**: permite garantizar una reproducción visual exacta (durabilidad)
 - **Obligatorio:**
 - Fuentes incrustadas (todas y completas)
 - Información de color independiente de dispositivo
 - Metadatos XMP
 - **Restricciones:**
 - Cifrado
 - Compresión LZW
 - Ficheros incrustados
 - Enlaces externos
 - Ficheros multimedia
 - Transparencia
 - Javascript

Accesibilidad

- PDF/A (ISO-19005-1)
 - Versión “reducida” del estándar PDF 1.4
 - **PDF/A-1a**: además de todo lo anterior (nivel acumulativo), fuerza que el documento sea **accesible**:
 - Tagged PDF (etiquetas)
 - Orden de lectura (estructura lógica del documento)
- Existe una gran variedad de herramientas de validación y conversión (aunque no hacen milagros)

Firma Electrónica

Firma Electrónica Avanzada vs. Reconocida

La Ley 59/2003 de Firma Electrónica especifica:

- (Art. 3.2) La **firma electrónica avanzada** es la firma electrónica que permite **identificar al firmante** y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que **ha sido creada por medios que el firmante puede mantener bajo su exclusivo control**
- (Art. 3.3) Se considera **firma electrónica reconocida** la firma electrónica avanzada basada en un **certificado reconocido** y generada mediante un **dispositivo seguro de creación de firma**

Firma Electrónica

- Alternativas
 - **XAdES/CAAdES** (estándares ETSI)
 - Recomendado por la EU
 - Estándar complejo (basado en XMLDsig)
 - El documento se “incrusta” dentro de un XML (base64)
 - Soporte de “sello de tiempo” (*timestamping*) avanzado, y **firmas longevas**
 - **Firma nativa PDF** (PKCS#7)
 - Estándar muy sencillo
 - La firma se integra en el propio documento
 - Soporte de “sello de tiempo” (*timestamping*)

Firma Electrónica

- Ventajas

- XAdES/CAAdES

- Sistema tecnológicamente más avanzado
 - Respaldo de la UE
 - No altera el documento original
 - Alguna implementación libre (OpenXades.org)
 - Firmas longevas (*timestamping* y evidencias de de los chequeos revocación)

Firma Electrónica

- Inconvenientes

- XAdES/CAAdES

- No existe una forma estándar de verificación (desempaquetado / validación)
 - **APPLET** → problemas !!!
 - Obligaría a disponer de dos versiones de cada documento (original y firmado) dado que la mayoría de usuarios no deseará lidiar con el desempaquetado / validación
 - Se baraja un sistema de validación “*server side*”, pero se descarta por cuestiones de “usabilidad” y “falta de garantías”

Firma Electrónica

- Ventajas

- **Firma nativa PDF (PKCS#7)**
 - Sistema de verificación de firma (OCSP incluido) integrado en los lectores más habituales (Acrobat Reader) → **no hay que desarrollar nada “client side”**
 - La firma se integra en el propio documento → **una única copia para todos**
 - Soporte de “sello de tiempo” (*timestamping*)
 - Amplia implantación (precedentes en otros Boletines en España)

Firma Electrónica

- Inconvenientes
 - **Firma nativa PDF** (PKCS#7)
 - Menos “avanzada”
 - Peor soporte para las “firmas longevas” → posibilidad de “re-firmado”

Se opta por la firma nativa PDF por la conveniencia de almacenar una copia única de los documentos PDF y proporcionar un interfaz uniforme (desde el punto de vista del usuario) para la verificación de la firma y la lectura habitual del Diario

- La integración de firma y *timestamping* se realiza a través de **iText** (Software Libre)

Firma Electrónica

- Con qué certificado firmar ???
 - El certificado usado deberá ser **verificable por el ciudadano**
 - Siguiendo las directrices del **Esquema de Identificación y Firma Electrónica** recién publicado por el MAP, se debería utilizar un certificado del tipo “**sello electrónico para la actuación automatizada**”, actualmente en fase de implantación por parte de las CAs reconocidas
 - Selección de **una o varias TSAs** para el “sello de tiempo” (*timestamping*)

Impacto en Sistemas y Comunicaciones

- El incremento de **ancho de banda** previsiblemente no será crítico, dado el actual **sobredimensionamiento** del caudal de Internet (2x100 Mbps + 1 Gbps)
- Se está estudiando que los ciudadanos utilicen **SSL para el acceso a la sede electrónica**
 - Descarga de labores de cifrado en los servidores web sobre los **balanceadores de carga**, de forma que sean estos los que terminen las conexiones SSL
 - El certificado de sede electrónica reside sobre los mencionados equipos (Cisco CSS 11506), dotados de una **tarjeta criptográfica** de propósito específico
- Se preveé un acceso “en claro” para *mirrors*, etc...

Impacto en el resto del Organismo

- Todo lo mencionado hasta aquí no supone más del 10% del impacto del proyecto
 - Grandes implicaciones a nivel organizativo / RRHH
 - A nivel de Tecnologías de la Información / Imprenta Nacional , se ha de rediseñar completamente el proceso de generación del Diario Oficial → **Nuevo Sistema de Producción (Composición y Montaje)**
- A estas alturas todavía hay cosas por decidir... !!!

DESEADNOS SUERTE !!!

(...y estén atentos a sus pantallas el próximo 1 de enero...) ☺



Gracias por su atención

David Guerrero

Dpto. Tecnologías de la Información

Boletín Oficial del Estado

<david@boe.es>