
CNIS
2016
VI CONGRESO NACIONAL
DE INNOVACIÓN
Y SERVICIOS PÚBLICOS
Transformación digital
al servicio de las personas
Madrid · 2 y 3 de Marzo

El contexto tecnológico de la firma electrónica

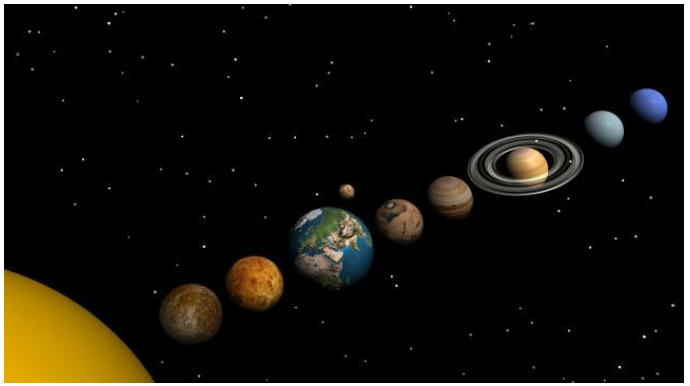
Daniel Sánchez Martínez (danielsm@um.es)
GT de e-Administración de CRUE-TIC

Contexto tecnológico de la firma electrónica

Navegadores y Java

- Estrategia durante la última década → integración de procesos de firma electrónica en navegadores
  - Ausencia de soluciones nativas generalizadas
  - Uso de componentes cliente Java
    - Acceso al almacén de certificados
    - Acceso a dispositivos criptográficos (DNIe)
    - Generación de formatos AdES
- Nivel de usabilidad decreciente
  - Actualizaciones frecuentes de navegadores y plug-in Java
  - Bloqueos de seguridad

Client e



Contexto tecnológico de la firma electrónica

Navegadores y Java

- El plug-in Java llega a su fin.
  - Google Chrome → abril y septiembre de 2015
  - Mozilla Firefox → final de 2016
  - Microsoft Edge → sin soporte
  - Oracle Java SE 9 → sin soporte (marzo de 2017)

¡¿alternativas?!

W3C W → e 2014
https://ww ryptoAPI/

- Se olvida del usc claves y tarjetas criptográficas
- https://www.yo m/watc NzTCoxr2ek

Firma cliente

Aplicaciones nativas

- Alternativa conservadora
  - Interacción con nuestros almacenes de certificados.
- DTIC - **Autofirm@**
  - Interacción con el navegador.
  - Script para sustituir el uso del miniapplet.
- **Aplicaciones ofimáticas**
  - Adobe, Microsoft, LibreOffice…
  - Facilitar el anexado de documentos ya firmados en formularios Web.

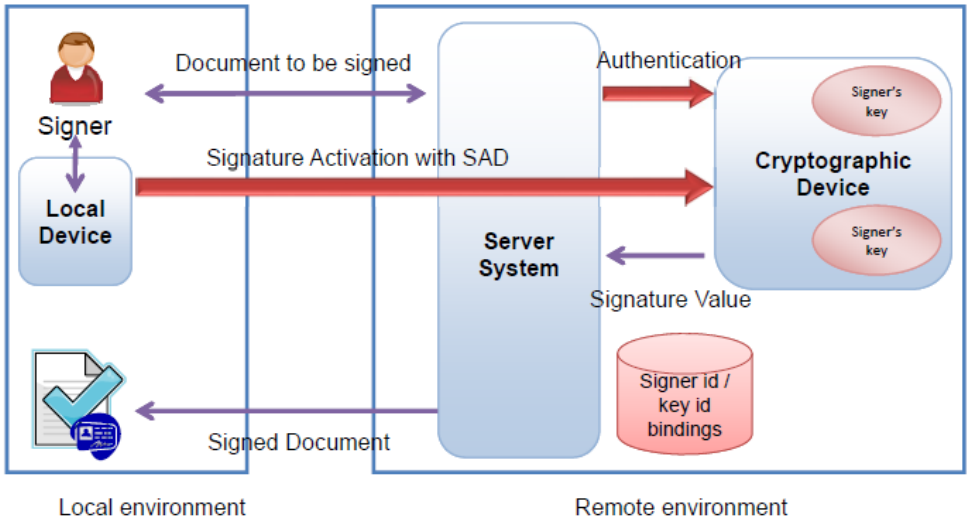
Firma cliente

Aplicaciones nativas

- **APPs móviles**
  - Certificado software instalado en el dispositivo.
  - Dispositivos Android con NFC → tarjetas criptográficas.
    - DNI 3.0
    - Tarjetas Universitarias
- **Debilidades**
  - Software adicional → soporte.
  - Provisión del certificado en cada dispositivo.

Firma centralizada

- **Características**
  - Regulados en el Reglamento eIDAS de la UE.
  - Centralización de claves en hardware criptográfico → modalidades *SaaS* y *On-premise*.
  - Garantía de control lógico exclusivo de las claves por parte del usuario.
  - Uso de segundos factores de autenticación → OTP al móvil.
  - Norma técnica CEN TS 419 241 → *Security Requirements for Trustworthy Systems Supporting Server Signing.*



Firma centralizada

- **Beneficios**
  - Gestión centralizada del ciclo de vida del certificado.
  - Capacidad para establecer políticas de uso en base a criterios operacionales.
  - Medidas de seguridad y auditoría detallada.
  - Simplificación de tareas de soporte → no requieren instalar software.
  - Integración mediante pasarelas y servicios de firma en la nube.
- **Ejemplos**
  - Cl@ve-Firma → ciudadanos
  - Plataformas para empleados públicos
- **Interrogantes**
  - ¿N servicios de firma centralizada = N integraciones independientes?
  - ¿Podría actuar Cl@ve como bróker de servicios de firma centralizada?
  - ¿Cuándo podrán generar firma electrónica cualificada (QES)?
  - ¿Aceptación psicológica del control exclusivo "lógico" –que no físico- de las claves?

Sistema de identificación como sistema de firma

Ley 39/2015 – Artículo 10.3

- *"3. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados."*
  - Ergo → Los sistema de clave concertada pueden ser admisibles como sistemas de firma electrónica.
  - Requiere regulación expresa
- **Interrogantes**
  - ¿Cómo acreditamos la autenticidad de la expresión de la voluntad y consentimiento cuando se usan claves concertadas?
  - ¿Qué evidencias se deben recoger? ¿Cómo se custodian y preservan? ¿Cómo se incluyen en un expediente electrónico? ¿Qué formatos utilizamos?
  - ¿Es razonable pensar en una NTI que establezca criterios comunes?
  - ¿Estas firmas podrían ser compatibles con el reglamento eIDAS?

Sistema de identificación como sistema de firma

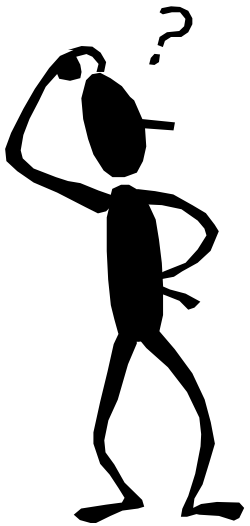
SGEE

- Normalización → Sistema de Gestión de Evidencias Electrónicas (SGEE)
  - Norma UNE 71505-2013.
  - Gestión de logs de actividades durante todo su ciclo de vida.
  - Establecimiento de medidas de seguridad.
  - Definición de formatos de intercambio.

Conclusiones

- Escenario complejo **sin una solución óptima** → todas presentan interrogantes y retos a abordar.
- Los sistemas de **firma electrónica centralizada** parecen prometedores, pero aún embrionarios.
- La prudencia invita a un **enfoque múltiple**, adecuado a cada contexto, trámite y colectivo de usuarios a los que se dirige.

¡ Gracias por su atención !



Daniel Sánchez Martínez (danielsm@um.es)
Grupo de Trabajo de Administración Electrónica
CRUE – Comisión Sectorial TIC (http://www.crue.org/TIC/)