Firma Electrónica

Introducción y conceptos básicos

www.atsistemas.com

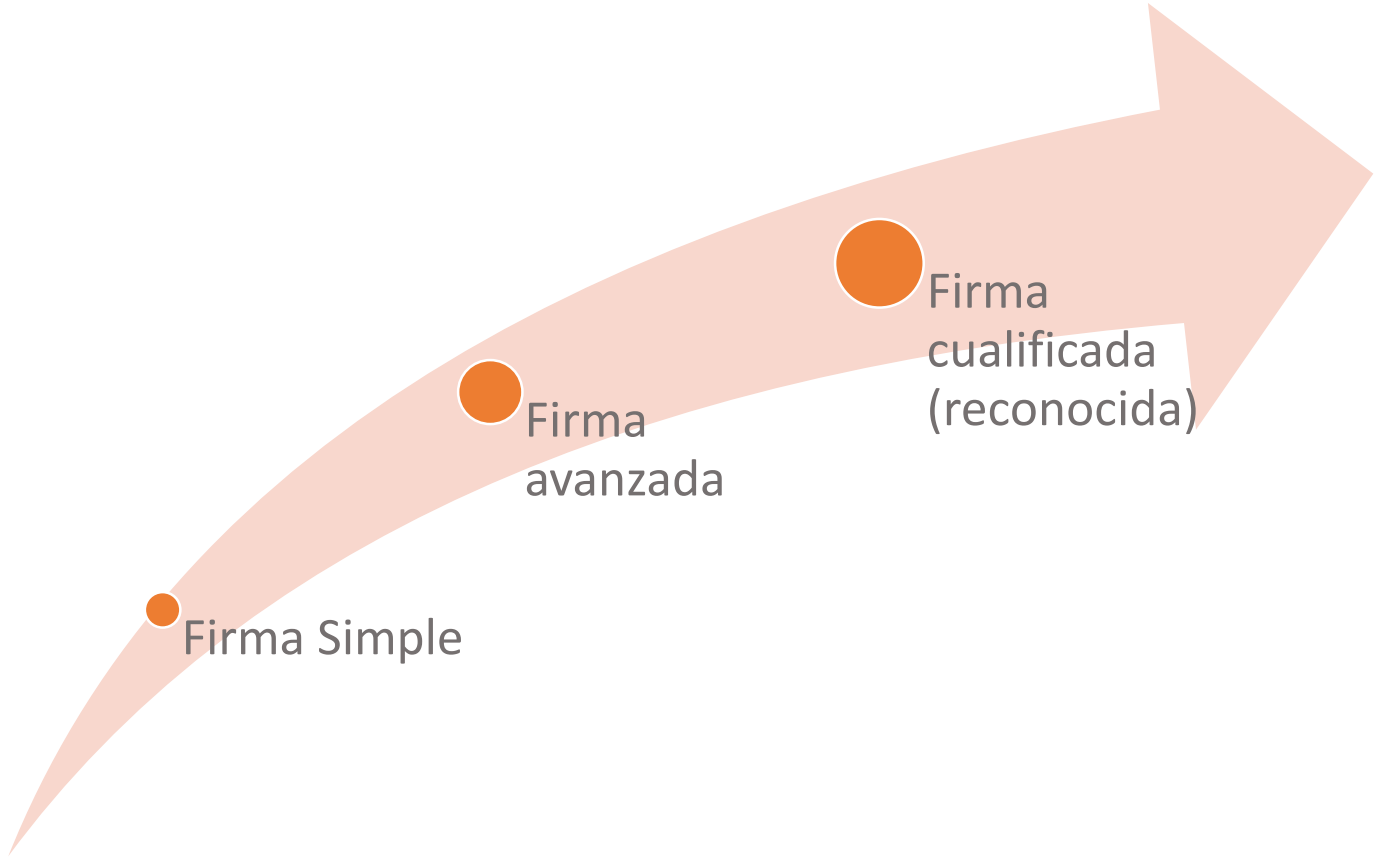
atsistemas
Consulting, IT Services & Software Development

Sobre el autor

- Tomás García-Merás
  - Más de diez años trabajando en Administración Electrónica, principalmente en proyectos de seguridad y firma electrónica.
  - Líder e impulsor de numerosos proyectos de firma electrónica y criptografía:
    - Cl@ve Firma (firma en la nube), AutoFirma (firma local), JMultiCard (controlador DNIe desarrollado en INTECO/INCIBE), etc.
  - Impulsor del Software Libre, tanto de su uso como de la generación de software con licencias abiertas.
  - Actualmente Gerente de Sector Público en atSistemas:
    - https://www.atsistemas.com/es

Introducción a la firma electrónica

- Pleno soporte legal desde 2003 (Ley 59/2003), reciente impulso por el reglamento europeo UE/910/2014.



Introducción a la firma electrónica

- Firma Simple
  - Cualquier cosa que consideremos firma.
    - Por ejemplo, el pulsar “Acepto” en un contrato o clausulado mostrado en una página.
- Firma Avanzada
  - 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.
- Firma cualificada (reconocida).
  - Es una firma avanzada hecha mediante un dispositivo cualificado de creación de firmas.
  - En caso de repudio, la carga de la prueba recae sobre el que cuestiona la validez de la firma.

Firma electrónica simple

- Ejemplos de Firma Simple
  - Firma típica de clausulado Web

Firma electrónica simple: Firma biométrica

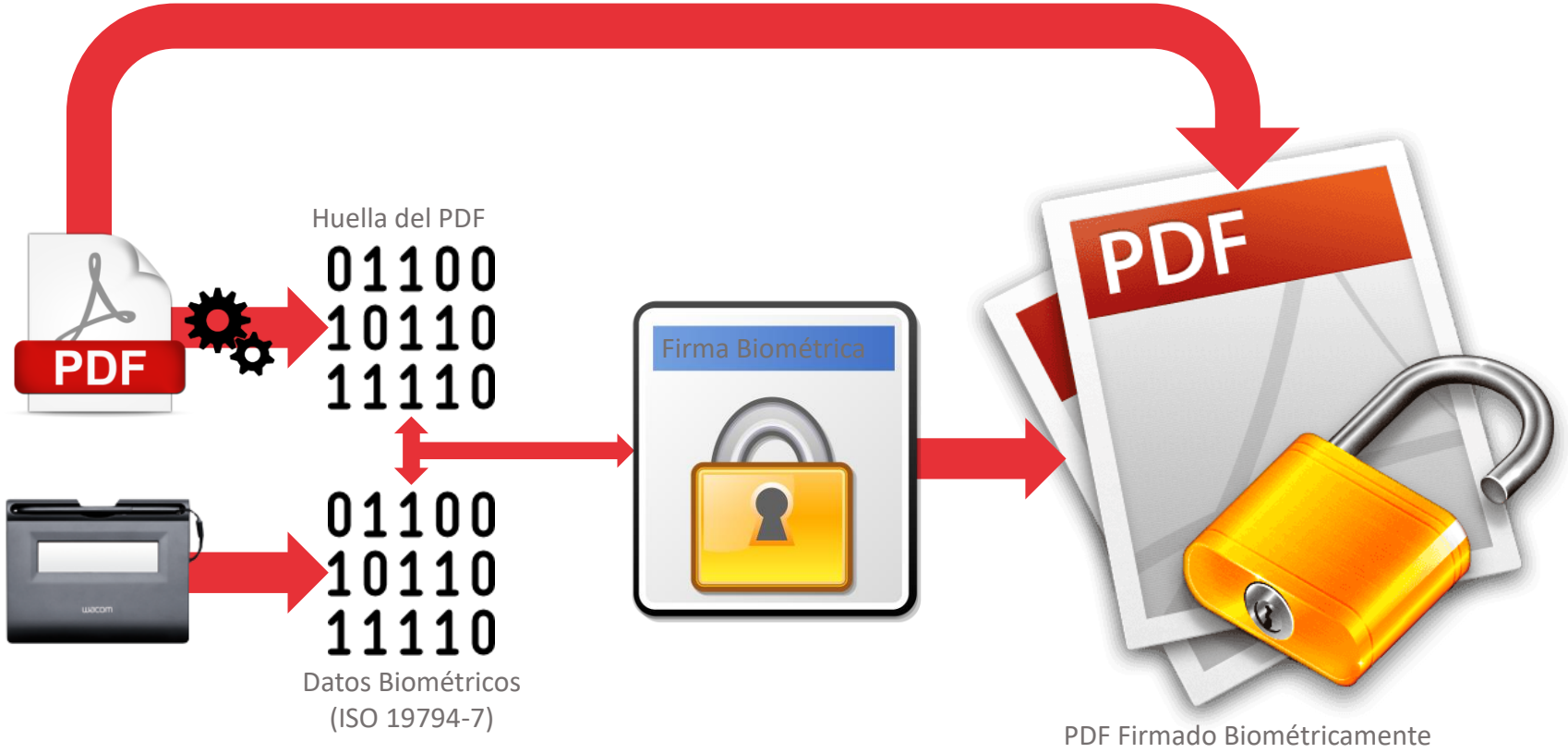
- Ejemplos de Firma Simple
  - Firma biométrica manuscrita

Firma electrónica simple: Firma biométrica

- Ejemplos de Firma Simple
  - Firma biométrica (manuscrita)
    - No se captura la “imagen” de la firma, sino sus rasgos biométricos (presión, velocidad, etc.), que se almacenan en un fichero ISO 19794-7.
      - Cuantos más rasgos se capturen, mayor es la vinculación la firma con el firmante:
        - Presión sobre la superficie,
        - Velocidad del trazo.
        - Inclinación del puntero.
        - etc.
      - Cuanto más natural sea el proceso de firma, mayor es la vinculación la firma con el firmante:
        - Uso de un puntero y no del dedo.
        - Firma en una posición normal de escritura.
        - Etc.
    - Es necesario un hardware de captura.
      - No todos capturan presión. Los que sí lo hacen:
        - USB o puerto serie (Windows y Linux): Wacom, Topaz, etc.
        - Tabletas y móviles: iPad con Apple Pencil o puntero Wacom Bluetooth, Samsung SPen (gama Note y otros modelos), etc.
        - Portátiles: Tecnología Windows Ink (Microsoft Surface, HP, etc.)

Firma electrónica simple: Firma biométrica

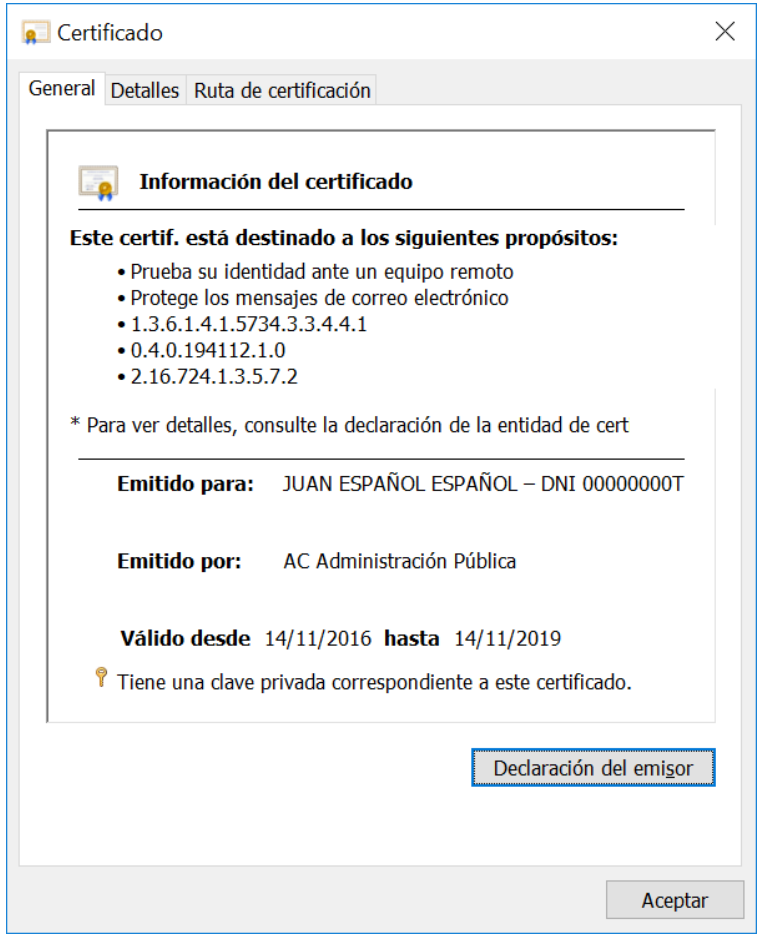
- Ejemplos de Firma Simple
  - Firma biométrica (manuscrita)
    - El proceso de la firma manuscrita



Firma electrónica simple: Firma biométrica

- Ejemplos de Firma Simple
  - Firma biométrica (manuscrita)
    - El proceso de la firma manuscrita:
      1. Se extraen los datos biométricos del firmante (en un formato normalizado ISO 19794-7).
      2. Se extrae la huella digital del PDF (en un formato normalizado, como SHA-512).
      3. Se juntan ambos, cifrándose de forma que solo un tercero de confianza pueda descifrarlo (este tercero custodiará la clave de descifrado, cargándonos un coste periódico por ello). Este paquete cifrado que contiene la huella del PDF a firmar y los rasgos biométricos del firmante constituye la firma biométrica.
      4. Se adjunta la firma biométrica al PDF.
      5. Un paso adicional, que si bien es opcional, es muy conveniente, es añadir un sello de tiempo al documento PDF firmado biométricamente.
         - Permite certificar el momento de la firma (mediante un tercero de confianza, la TSA).
    - ¿Cómo se verifica una firma biométrica?
      - El custodio de la clave extrae datos biométricos y huella del PDF.
        - Este acto tiene un coste (pocos cientos de euros).
      - Se comprueba que la huella del PDF coincide (integridad del documento firmado).
      - Un perito caligráfico verifica si los datos biométricos corresponden realmente con el firmante.
        - No nos dirá “sí” o “no”, sino una probabilidad de “sí” (suele ser cercana al 90%).
      - Una autoridad (por ejemplo, un juez) determina finalmente la validez de la firma en base a las evidencias aportadas.
        - La evidencia principal es el informa pericial, pero podemos aportar otras adicionales.

Firma electrónica avanzada



- Firma avanzada: Certificados
  - Si bien hay disparidad de opiniones, podemos decir que la firma avanzada es aquella basada en certificados digitales.
    - Un certificado digital lo emite una Autoridad de Certificación (CA), que puede ser reconocida o no.
      - Evidentemente, su validez varía si no lo es.
    - Una CA reconocida re apoya siempre en una Autoridad de Registro (RA), que verifica la identidad de los titulares de los certificados.
      - La CA y la RA pueden ser la misma entidad.
      - Una RA puede instalar una oficina de registro en las instalaciones de una empresa para registrar a sus empleados (de hecho, es lo normal).
      - El registro, normalmente, hay que repetirlo periódicamente (suele ser cada 8 años).
    - Hay distintos tipos de certificados:
      - Personal.
        - **Ya no existe el certificado de persona jurídica.**
      - De representante de empresa.
      - De pertenencia a empresa.
      - De sello electrónico de órgano (sector público).
      - Otros (empleado público, de sede, etc.).
    - La emisión de un certificado puede acarrear un coste.
    - El registro del titular puede acarrear un coste.

Firma electrónica avanzada

- Firma avanzada AdES (formato normalizado europeo de firma avanzada)
  - Distintos formatos, para cualquier uso:
    - XAdES: XML, fácil de procesar en sistemas informáticos.
    - CAdES: Binario, compacto y eficiente.
    - PAdES: En PDF. El usuario, con Adobe Reader, puede ver y comprobar las firmas de un documento.
    - Otros formatos: OOXML (variante “no oficial” de XAdES), para firma de MS-Office (Word, Excel, etc.).
  - Carece de los problemas de la firma simple: Una firma lo es de un firmante y para un documento único, y no hay vulnerabilidades que permitan cambiar esto.
  - La firma electrónica avanzada es fundamental para la transformación digital, ya que nos permite eliminar por completo el papel.
    - Contratos, albaranes, facturas, actas… Cualquier cosa que necesite o se refuerce con una firma.
  - Hay procesos de pasar de papel a electrónico documentos firmados:
    - Digitalización certificada.

Firma electrónica cualificada

- Firma cualificada.
  - Es la firma avanzada que se realiza en un “Dispositivo Cualificado de Creación de firmas”, estando la clave privada siempre bajo el control de su titular.
  - Dos tipos básicos: Firma local y firma en la nube.
    - En la firma local el firmante custodia su propia clave de firma, preferentemente en un “dispositivo seguro de creación de firmas” (SSCD), como una tarjeta inteligente (DNIe, etc.), un USB criptográfico, etc.
    - En la firma en la nube es un tercero de confianza (un PSC) el que nos custodia la clave y firma por nosotros.
  - Firma local:
    - En su variante más segura (firma reconocida), es equivalente a una firma ante notario (requiere que la clave resida en un SSCD reconocido, como el DNIe).
    - Los certificados no pueden usarse directamente para firma en Web, por lo que necesitamos aplicaciones como Applets de Java, controles ActiveX o aplicaciones tipo AutoFirma.
    - Hay bibliotecas de software libre para realizar estas firmas: @firma.
      - Es la base de muchos productos de firma electrónica:
        - Casi toda la infraestructura de firma del Gobierno de España (desde Red.es hasta los más pequeños ayuntamientos, pasando por el Ministerio de Hacienda y Función Pública, la AEAT, la Junta de Andalucía…).
  - Firma en la nube:
    - Un tercero custodia nuestras claves y firma por nosotros. El firmante autoriza mediante un OTP (SMS, etc.).
    - El proveedor de servicios de firma en la nube provee un API de servicios Web para su uso.
    - Hay un middleware de integración estándar (software libre) que se perfila como estándar de facto: FIRe
      - Promovido por FNMT-RCM, Gerencia de Informática de la Seguridad Social, Cuerpo Nacional de Policía y Ministerio de Hacienda y Función Pública.
      - En uso por muchas administraciones públicas.

Firma electrónica en la nube

- La firma electrónica en la nube permite eliminar las complejidades de la firma electrónica local (aplicaciones nativas, Applets, etc.). Al proporcionarse el servicio mediante servicios Web, es posible integrar con facilidad la firma electrónica en cualquier proceso.
- Un API estándar (software libre): “Cl@ve Firma” (ahora llamado FIRe).
  - FIRe / Cl@veFirma permite usar distintos PSC de firma en la nube (por ahora GISS/CNP y FNMT, en breve otros prestadores).
  - Es posible la provisión de la capa de integración también en la nube (AWS, etc.).
  - Integración final en Java, PHP o .NET.
- Una enorme oportunidad en cualquier sector.
  - La firma en la nube es una novedad del reglamento eIDAS. Está en su fase temprana, hay grandes empresas que pueden beneficiarse de su adopción.

Ejemplos de firma electrónica

- Firma de ciudadano (sector público) para trámites electrónicos.
  - Infinidad de ejemplos.
- Contratación vía Web:
  - Contratación de “activos digitales” que necesiten un contrato firmado.
- Firma en procesos burocráticos internos:
  - Cualquier organización, especialmente en el sector público.
- Sistemas portafirmas:
  - Un sistema portafirmas es el que permite distribuir los documentos para su firma, proporcionado los mecanismos para esta, definiendo los circuitos de firma (los flujos documentales).
    - Definen distintos tipos de actos de firma (contrafirma, visto bueno, firma, etc.).
    - Permiten la firma desde dispositivos móviles.
- Otros proyectos.
  - Seguridad lógica y jurídica en los API.
  - Cifrado de datos.
  - Etc.

GRACIAS

www.atsistemas.com

902 888 902

Madrid
C/Valle de Alcudia.3 Edificio 2,
planta 1. 28232. Las Rozas, Madrid

Barcelona
Passeig de Grácia 55, 8º - 4ª
08007, Barcelona

Cádiz
Edificio Jerez Parque Empresarial,
Calle del Desarrollo 2; oficina 12,
planta 1, 11047, Jerez de la Frontera

Zaragoza
Centro Tecnológico TIC XXI C/Bari,
57 Plataforma Logística (PLA-ZA),
50197, Zaragoza

A Coruña
Edificio Mans, Polígono de Pocomaco,
parcela D22, 15190