Firma Digital XML:

XMLdSig: W3C-XML Signature Syntax and Processing
W3C Recommendation 10 June 2008
Funcionalidad básica para firma digital de varios objetos al mismo tiempo.
Medio básico para incorporar cualquier tipo de información calificada que se necesite.

```
<Signature>                     -- Firma digital sobre un documento
  <SignedInfo>                  -- Informacion a la que se le va a aplicar el algoritmo de Firma Digital
        <SignatureMethod/>      -- Algoritmo a utilizar para la firma digital de <SignedInfo>
        <CanonicalizationMethod/>-- Algoritmo de Canonicalizacion a utilizar en <SignedInfo> antes de la firma digital
        <Reference URI="XXX1">  -- Referencia al documento o elemento dentro del documento que se desea firmar
                <Transforms/>   -- Algoritmos de Transformación antes de calcular el Digest
                <DigestMethod/> -- Algoritmo de Digest o hash o "resumen criptográfico" sobre el documento ya transformado
                <DigestValue/>  -- Valor hash calculado sobre el documento a firmar en Base64
                                -- (Permite verificar que el documento no ha cambiado)
        </Reference URI="XXX2">
        <Reference/>*           -- Permite firmar varios documentos o fragmentos con una sola firma
  </SignedInfo>
  <SignatureValue/>             -- Valor de la firma digital sobre <SignedInfo> en Base64
                                -- (Permite verificar la autenticidad del firmante,
                                -- que el SignedInfo no haya cambiado y por tanto el documento original tampoco)
  <KeyInfo/>?                   -- Llave pública o Certificado del firmante
  <Object/>*                    -- Documento a firmar en caso de firma envolvente (Enveloping Signature).
</Signature>
```

ETSI TS 101 903 V1.4.1 (2009-06)
Technical Specification
XML Advanced Electronic Signatures (XAdES)

El XAdES agrega restricciones y extiende el formato XMLdSig, incorpora informacion adicional necesaria para asegurar la validez en el momento de la firma, aun cuando el firmante o alguna parte validadora lo quisiera repudiar en el futuro.
Se usan timestamps o timemarks (almacenamientos confiables) para probar la validez de la firma en el futuro.
Tambien se pueden usar timestamps adicionales para proteger a largo plazo posibles rupturas de la llaves o debilidades de los algoritmos en el futuro

XAdES define 6 perfiles (formas) según el nivel de protección ofrecido. Cada perfil incluye y extiende al previo:

XAdES-BES, forma básica que hace disponible la cadena de certificacion, indicando sin ambiguedades el certificado firmante, y califica cada documento firmado
XAdES-EPES, forma básica a la que se la ha añadido información sobre la política de firma,
XAdES-T (timestamp), añade un campo de sellado de tiempo para proteger contra el repudio,
XAdES-C (complete), añade referencias a datos de verificación (certificados y listas de revocación) a los documentos firmados para permitir verificación y validación off-line en el futuro (pero no almacena los datos en sí mismos),
XAdES-X (extended), añade sellos de tiempo a las referencias introducidas por XAdES-C para evitar que pueda verse comprometida en el futuro una cadena de certificados,
XAdES-X-L (extended long-term), añade los propios certificados y listas de revocación a los documentos firmados para permitir la verificación en el futuro incluso si las fuentes originales (de consulta de certificados o de las listas de revocación) no estuvieran ya disponibles,
XAdES-A (archivado), añade la posibilidad de timestamping periódico (por ej. cada año) de documentos archivados para prevenir que puedan ser comprometidos debido a la debilidad de la firma durante un periodo largo de almacenamiento.

ETSI TS 103 171 V2.1.1 (2012-03)
Electronic Signatures and Infrastructures (ESI);
XAdES Baseline Profile

Define 4 niveles de aceptación (BASELINE):
- B-Level (Nivel Basico)
- T-Level (Trusted time for signature existence)
- LT-Level (Long Term level)
- LTA-Level (Long Term with Archive time-stamps)

Digital Signature Service (https://joinup.ec.europa.eu/software/sd-dss)
version : 4.6.0 - 2016-02-22

“Old levels: -BES, -EPES, -C, -X, -XL, -A are not supported any more when signing”