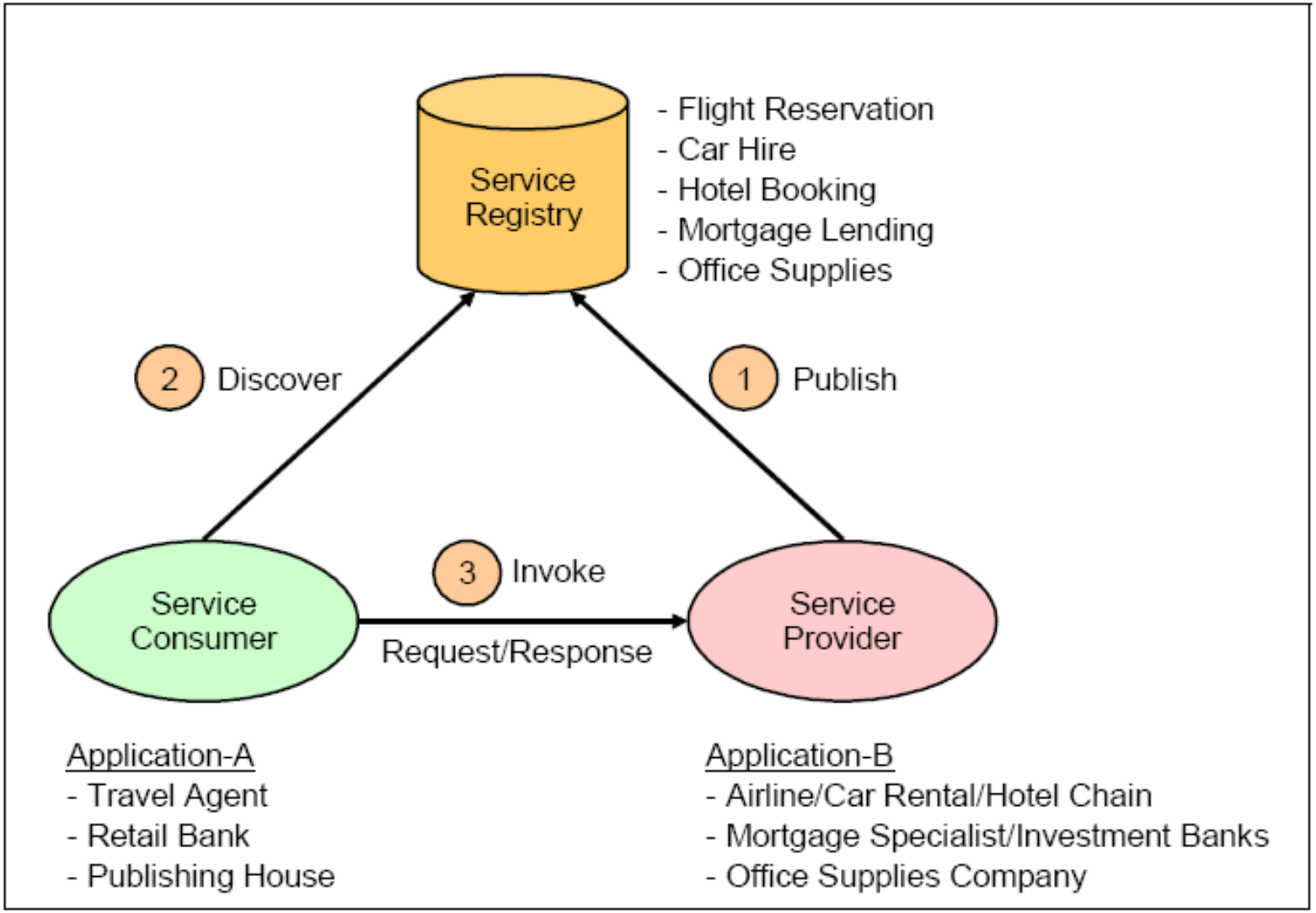
Firma Digital

Agenda

- Introducción a SOA (***S**ervice **O**riented **A**rchitecture)*
- SOAP (*Simple Object Access Protocol)* - Security
- XML - Signature
- Métodos de Canonicalización
- WS-Security
- Como Firmar Digitalmente un documento

- SOA es un framework conceptual para el desarrollo de aplicaciones que vinculen la infraestructura IT con la logica del negocio
- Consta de tres elementos que interactuan:
  - Service Provider (proveedor)
  - Service Broker (intermediario)
  - Service Consumer (consumidor)
- La arquitectura se caracteriza por el **bajo acoplamiento** entre estas entidades


Service Registry
- Flight Reservation
- Car Hire
- Hotel Booking
- Mortgage Lending
- Office Supplies
2 Discover
1 Publish
3 Invoke
Request/Response
Service Consumer
Service Provider
Application-A
- Travel Agent
- Retail Bank
- Publishing House
Application-B
- Airline/Car Rental/Hotel Chain
- Mortgage Specialist/Investment Banks
- Office Supplies Company

Componentes de SOA

- **XML** es un lenguaje para describir informacion estructuradamente pero independientemente de la representacion
- **SOAP** es una especificacion que regula el intercambio de mensajes estructurados, en formato XML. Un mensaje SOAP contiene:
  - **Envelope –(Sobre)**
  - **Encabezado-(Header)**
  - **Cuerpo-(Body)**

SOAP

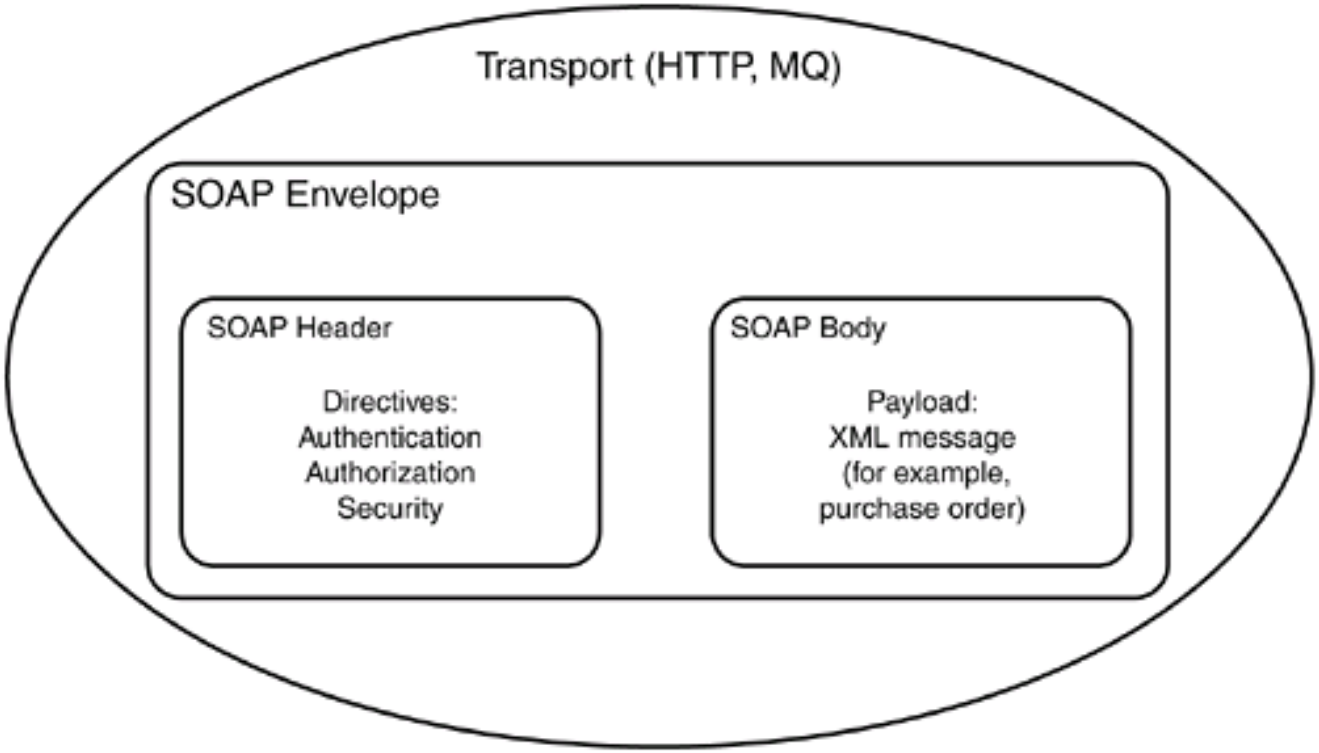
- Se creó como una forma de transporte en XML de un ordenador a otro a través de una serie de protocolos estándar de transporte.

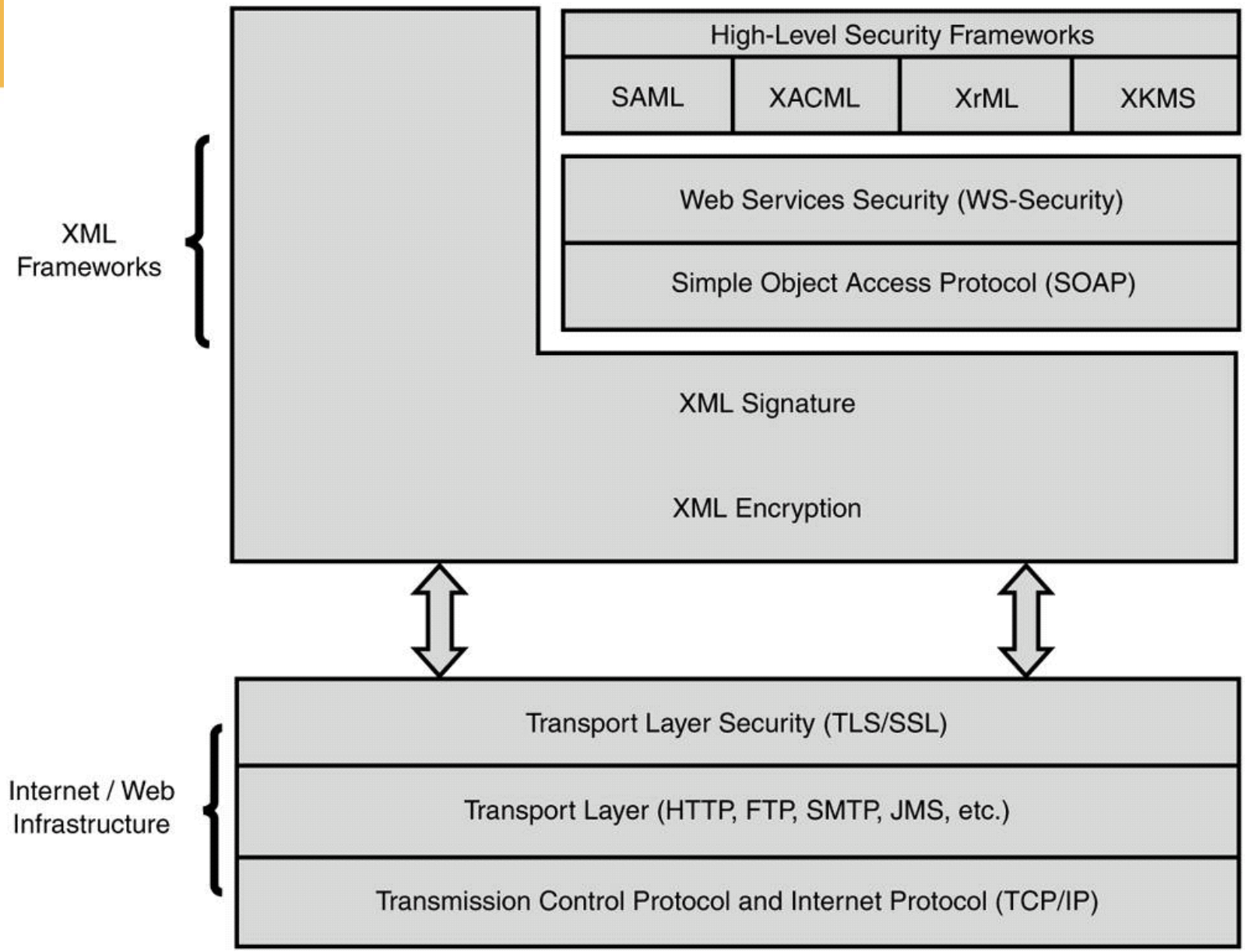
HTTP es el más común de los protocolos de transportes y, por supuesto, es el más utilizado en la Web

SOAP proporciona un mecanismo de forma simple, coherente y extensible mecanismo que permite que una aplicación pueda enviar un mensaje XML a otro.

SOAP es lo que hace posible integración de aplicaciones, porque después que XML define el contenido de un mensaje, es SOAP el que se encarga de mover los datos de un lugar a otro de la red

SOAP


Transport (HTTP, MQ)
SOAP Envelope
SOAP Header
Directives:
Authentication
Authorization
Security
SOAP Body
Payload:
XML message
(for example,
purchase order)


High-Level Security Frameworks
SAML
XACML
XrML
XKMS
Web Services Security (WS-Security)
Simple Object Access Protocol (SOAP)
XML Frameworks
XML Signature
XML Encryption
Transport Layer Security (TLS/SSL)
Transport Layer (HTTP, FTP, SMTP, JMS, etc.)
Transmission Control Protocol and Internet Protocol (TCP/IP)
Internet / Web Infrastructure

Consorcio World Wide Web (W3C)

- El Consorcio World Wide Web (http://www.w3.org/Consortium/) se fundó en Octubre de 1994 para liderar el WWW a su máximo potencial mediante el desarrollo de protocolos comunes que fomenten su evolución y aseguren su interoperabilidad.

- El W3C tiene alrededor de 400 organizaciones miembro procedentes de todo el mundo y ha alcanzado un reconocimiento internacional por su contribución al crecimiento de la Web.

XML - Signature

- XML-Signature Syntax and Processing
- Recommendación del10 de Junio de 2008

- Este documento especifica la firma digital XML y reglas de procesamiento de la sintaxis. La Firmas en XML proporciona integridad, la autenticación de mensajes y / o servicios de autenticación de datos de cualquier tipo, ya sea situada en el XML, o en cualquier otro lugar.

Objetivos

- Asegurar que un mensaje no ha sido alterado o manipulado . (integritegridad)
- Proporcionar un medio para que en la auditoría el mensaje no puedea ser repudiado . (autenticidad del firmante)

Structure

- <Signature>
- <SignedInfo>
- <CanonicalizationMethod/>
- <SignatureMethod/>
- (<Reference URI? >
- (<Transforms>)?
- <DigestMethod>
- <DigestValue>
- </Reference>)+
- </SignedInfo>
- <SignatureValue>
- (<KeyInfo>)?
- (<Object Id?>)*
- </Signature>

El atributo URI es opcional e identifica el objeto de datos que debe ser firmado. Este atributo se podría omitir a lo sumo en un elemento *Reference* dentro del mismo elemento *Signature*

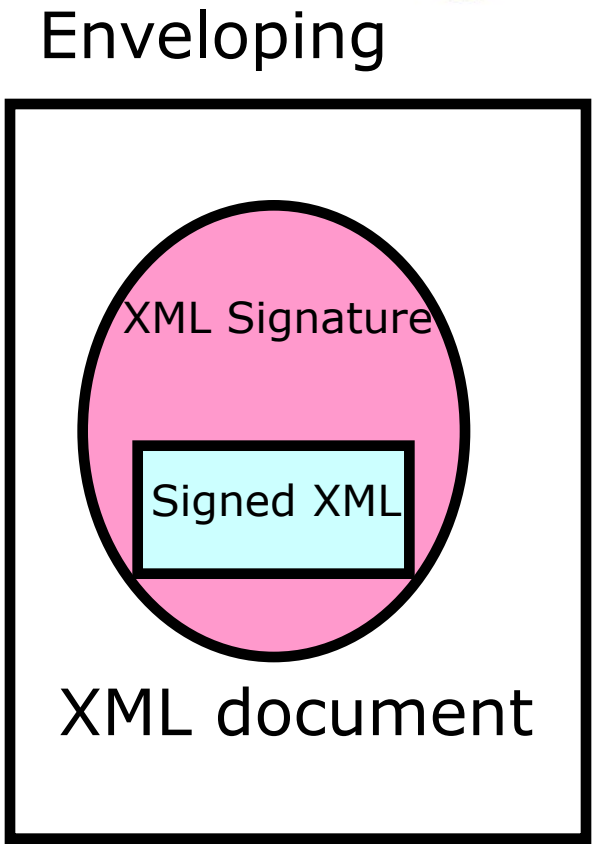
El elemento *KeyInfo* indica la clave (o información que permite al receptor del mensaje conocerla) que debe ser utilizada para validar la firma.

Las firmas digitales XML se representan mediante el elemento *Signature* que posee la siguiente estructura (donde '¿' significa 1 ó mas ocurrencias y '* ' significa 0 ó más ocurrencias):

xmlns="http://www.w3.org/2000/09/xmldsig#"

Tipos de Signatures

- Enveloping Signature
  - El dato vive dentro de la estructura XML signature
  - Bueno para la firma de datos que se están envasados en la carga útil del XML

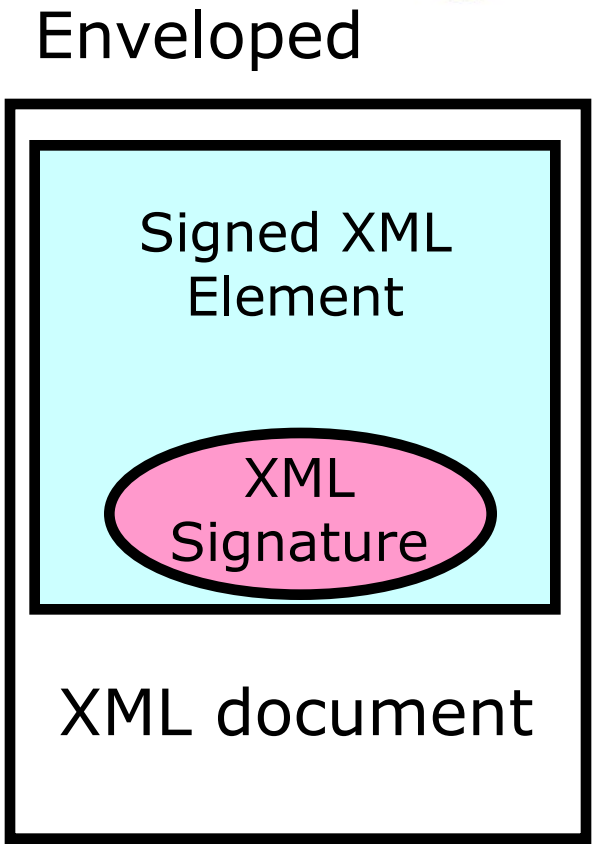


Enveloping Signature

```
<?xml version="1.0"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
                Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
    20010315"/>
    <SignatureMethod
              Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-
    sha1"/>
    <Reference URI="#myobj">
      <DigestMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>C2g9BLcGyGPCVKuF2byR1Ym+6pE=</DigestValue>
    </Reference>
  </SignedInfo>
   <SignatureValue>+R/XEOHDvR/jbmmpiuH4ZcRqC6c=</SignatureValue>
  <Object Id="myobj">Hello World!</Object>
</Signature>
```

Types of Signatures

- Enveloped Signature
  - Los Datos viven fuera y contienen la estructura de XML siganture
  - Bueno para la firma de partes o la totalidad de un documento XML

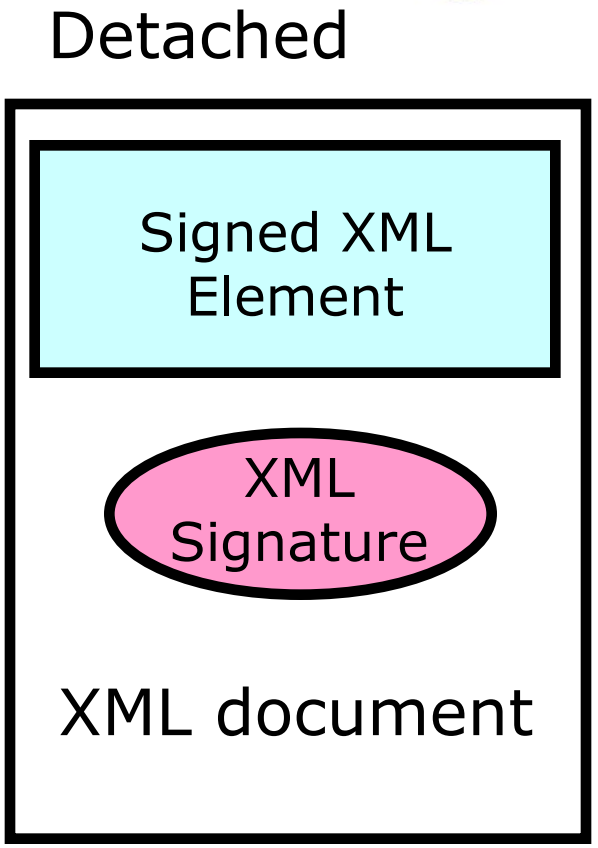


Enveloped Signature


```
<?xml version="1.0"?>
<Envelope>
  <Data>content</Data>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
    <Reference>
      <Transforms>
        <Transform
            Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>MMMkB0ZPp82XrUvJMFqDIEuXy0o=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>mVPvfcVSXi9elKL+IcSCAzD4Jbk=</SignatureValue>
</Signature></Envelope>
```

Types of Signatures

- Detached Signature
  - Los datos viven fuera y no contiene la estructura XML signature
  - Los datos pueden residir en un lugar remoto direccionable por URI



Ejemplo de Detached XML Signature

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig# ">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference URI="http://www.w3.org/TR/xml-stylesheet">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>60NvZvtdTB+7UnlLp/H24p7h4bs=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>
  juS5RhJ884qoFR8flVXd/rbrSDVGn40CapgB7qeQiT+rr0NekEQ6BHhUA8dT3+BC
  TBUQI0dBjlml9lwzENXvS83zRECjzXbMRTUtVZiPZG2pqKPnL2YU3A9645UCjTXU
  +jgFumv7k78hieAGDzNci+PQ9KRmm//icT7JaYztgt4=
  </SignatureValue>
  <KeyInfo>
    <X509Data>
      <X509IssuerSerial>
        <X509IssuerName>CN=Test RSA CA,O=Baltimore Technologies\,
Ltd.,ST=Dublin,C=IE</X509IssuerName>
        <X509SerialNumber>970849928</X509SerialNumber>
      </X509IssuerSerial>
    </X509Data>
  </KeyInfo>
</Signature>
```

Generación de firma paso a paso

- Para cada elemento
  - Aplicar las transformaciones necesarias
  - Calcular el hash para el output de la transformación
  - Guardar el hash en DigestValue
- Canonicalizar el elemento SignedInfo
- Calcular el hash del SignedInfo canonicalizado
- Firmar el hash de SignedInfo con mi clave privada y guardarlo en SignatureValue
- Agregar la información de la clave en KeyInfo
- recorger SignedInfo, SignatureValue, KeyInfo dentro de Signature

Verificación de la firma Paso a Paso

- Canonicalizar el SignedInfo
- Realizar el hash de SignedInfo
- Verificar la firma en SignedInfo
  - Verificar el valor de la firma con la clave pública
  - Verificar la veracidad de la clave pública
- Para cada elemento de referencia que fue firmado
  - Aplicar las transformaciones necesarias
  - Calcualr el digesto de la salida de la trasforamción
  - Verificar si el hash que calculamos es igual al valor que está en DigestValue

XML Signature Algoritmos Cryptograficos

- Funciones de Hash
  - **SHA-1**, SHA-256, SHA-384, SHA-512, MD-5
- Métodos de firma asimétricos
  - **RSA with SHA-1**, SHA-256, SHA-384, SHA-512, MD-5
  - DSA with SHA-1, SHA-256, SHA-384, SHA-512, MD-5
- Methodos de firma simétricos
  - **HMAC with SHA-1**, SHA-256, SHA-384, SHA-512, MD-5

XML Signature – Opciones de Key Info

- Clave Asimétrica
  - Key Name
  - Key Value
    - RSA
      - » Modulus, Exponent
    - DSA
      - » P,Q,Y,G
  - X509 Data
    - Certificado
    - Issuer/Serial
    - Subject Key Identifier
    - Subject Name
- Clave Simétrica
  - Key Name

▪Métodos de Canonicalización

Un espacio en blanco dentro de un elemento XML no tiene ninguna significancia sintáctica, de forma que <Elemento> es sintácticamente idéntico a <Elemento >, que incluye un espacio en blanco antes del carácter “>”. Como la firma digital se crea usando un algoritmo de clave asimétrica para codificar el resultado de hacer pasar el documento XML serializado por una función de hash, un único byte de diferencia haría que la firma digital variara.

Para evitar este problema y garantizar que documentos XML idénticos en sentido lógico produzcan firmas digitales idénticas, se suele emplear una transformación de canonización XML.

▪XML - Signature

▪Métodos de Canonicalización

- La especificación W3C XML Digital Signature define dos métodos de normalización de la información que es firmada: XML Canonicalization y XML Exclusive Canonicalization. El primer método se conoce también como el método de normalización inclusivo mientras que el segundo se conoce como el método de normalización exclusivo.

- El primero guarda relación con la equivalencia lógica entre documentos XML estructuralmente distintos. Dos documentos XML que no son absolutamente idénticos byte a byte podrían ser lógicamente equivalentes y es deseable que ambos produzcan la misma firma digital octeto a octeto.

- El segundo problema es que las firmas digitales podrían desear firmar datos como xx:foo. El significado de xx:foo podría cambiar si el espacio de nombres fuera redefinido y, por tanto, la firma digital no debería ser igual si el espacio de nombres se redefine

C14N – Prefijos del Namespace

- Los Prefijos son significantes
- <n1:a xmlns:n1="www.intel.com">foo bar</n1:a>
- No es lo mismo que
- <n2:a xmlns:n1="www.intel.com">foo bar</n2:a>
- Debido a que los prefijos pueden ser embebidos dentro de texto/atributo valor
- <n1:a xmlns:n1=www.intel.com language="n1:english">foo bar</n1:a>
- <n2:a xmlns:n2=www.intel.com language="n1:english">foo bar</n2:a>
- Canonicalización preserva el prefijo del namespace

Métodos de Canonicalización

- Inclusive Canonicalization
  - Todos los nombres de los nodos en un ápice elemento se considera que tienen un efecto y aparecen en el nodo-conjunto
- Inclusive Canonicalization With Comments
  - Igual que el anterior, nodos comentados se incluyen en la salida
- Exclusive Canonicalization
  - El nodo de Namespace es considerado para tener un efecto y aparece en la salida donde el prefijo es visible en el nombre del elemento o en le nombre del atributo
  - Es el método más utilizado
- Exclusive Canonicalization With Inclusive List
  - Los namespace de los nodos son tratados como se especifica en Inclusive Canonicalization cuando el aparato esté especificado en la Inclusive List y como Exclusive Canonicalization

C14N Input Rules

- Eliminar la declaración XML y de DTD
- Sustituir entity/character referencias con definiciones
- Convertir lineas rotas en x0A
- Eliminar secciones CDATA
- Normalizar attributo valor
  - Todas las líneas rotas son normalizadas
  - Comenzar con un valor vacío normalizado
  - Para cada caracter , entidad ref, char ref
    - Todos los caracteres referenciados son reemplazados
    - Reemplazar las entidades referenciadas y recurrentemente aplicar este paso
    - Por cada caracter espacio en blanco, tab horizontal, nueva línea, retorno de carro o espacio, añadir un carácter de espacio para el valor normalizado
  - Si el tipo de atributo no es CDATA, descartar los principales caracteres de espacio y los rezagados, y reemplaza cualquier secuencias internas del espacio con un único carácter de espacio

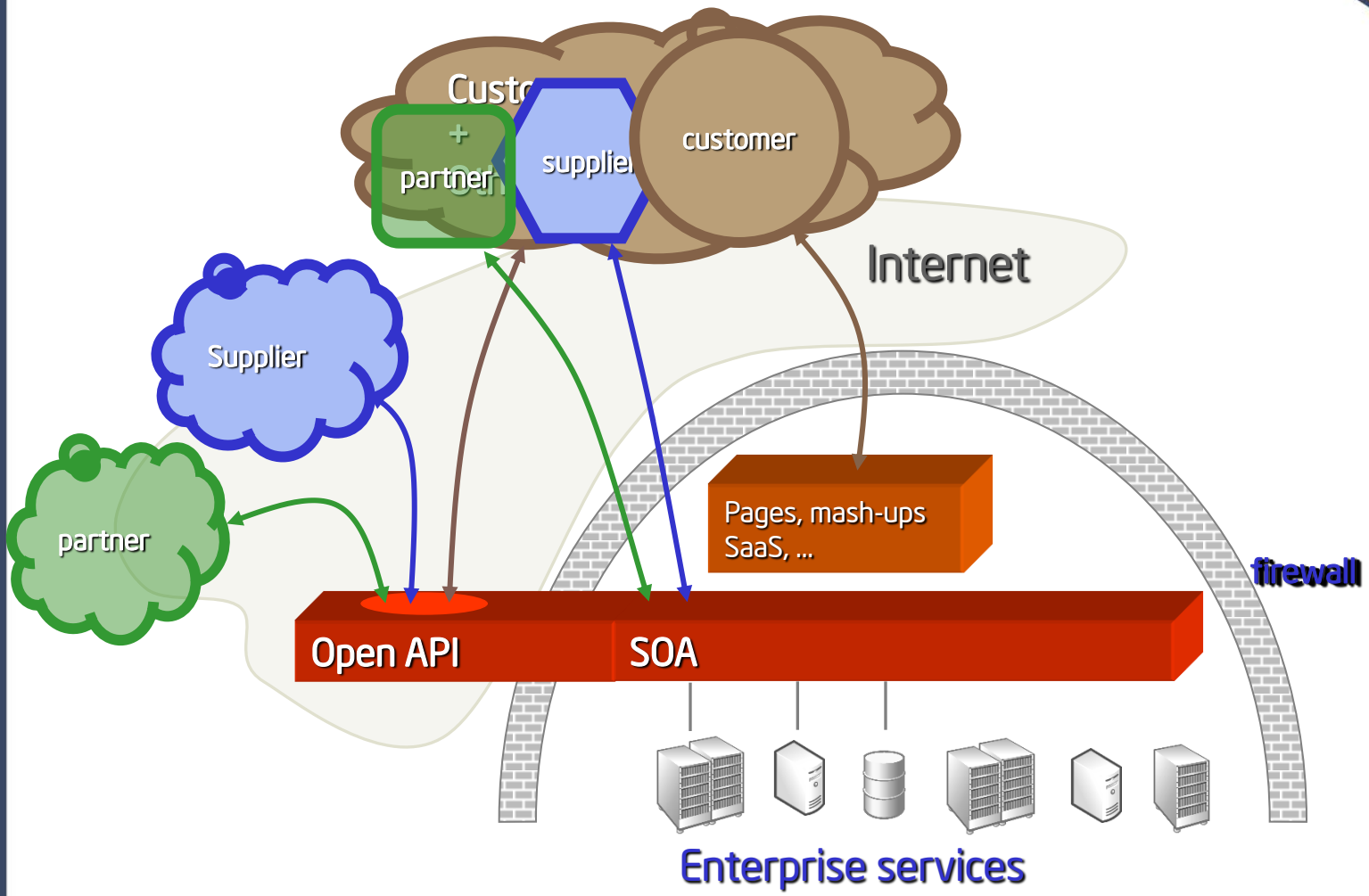
OASIS (Organization for the Advancement of Structured Information Standards)

OASIS en un consorcio global sin fines de lucro que conduce el desarrollo, convergencia y uso de estándares en el comercio electrónico (e-business)

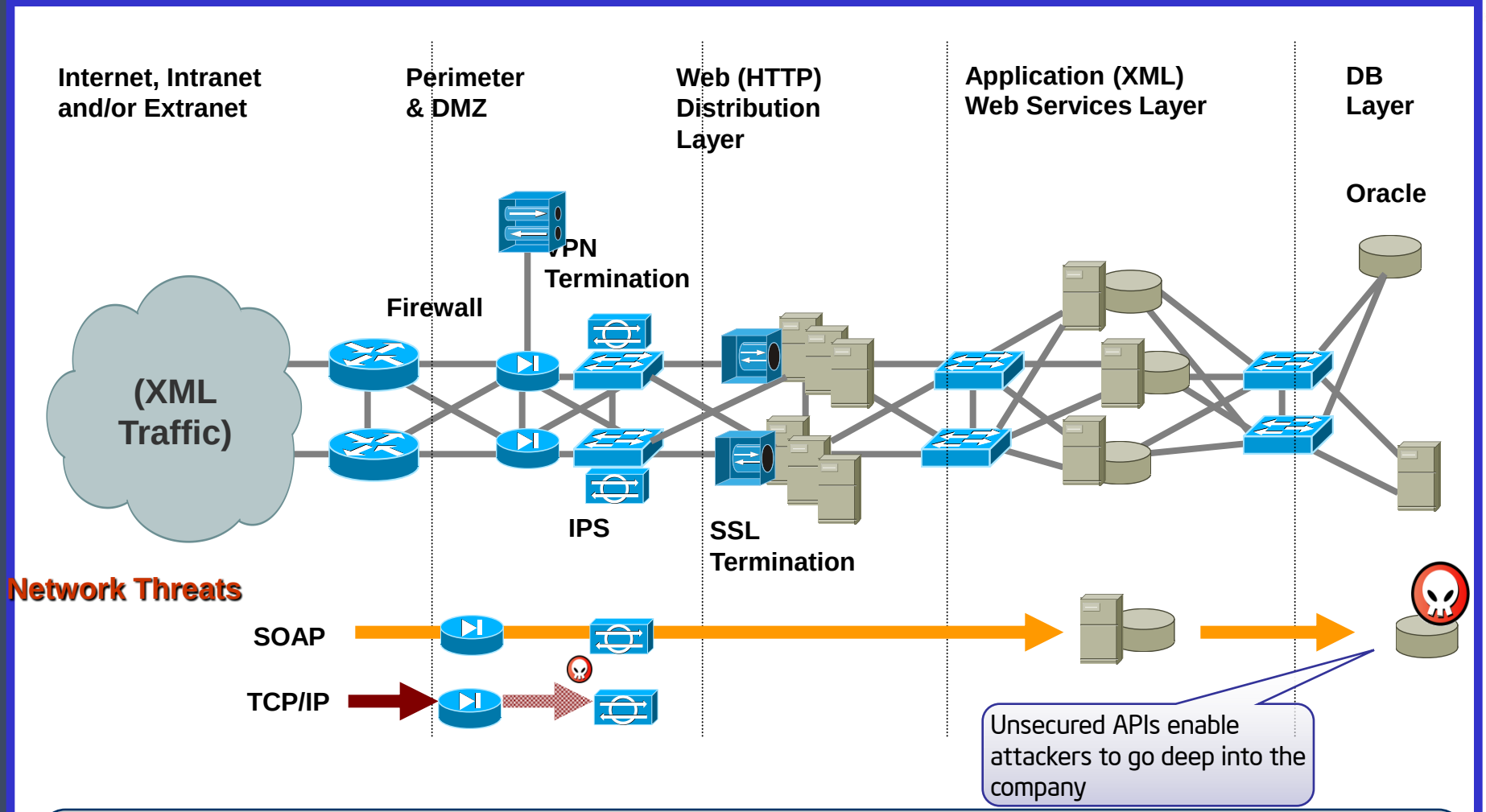
OASIS se componen de más de 600 corporaciones y miembros individuales ubicados en más 100 países repartidos por todo el mundo.

https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

WS - Security


customer
partner
Internet
Supplier
partner
Pages, mash-ups
SaaS, ...
firewall
Open API
SOA
Enterprise services

WS - Security



Perimeter defense is not enough, WS-Security can help with data integrity and authentication

Anatomy of the SOA Security challenge

The need for end to end security

Today's technologies like SSL do not provide end to end protection

John Doe

```
<XML>
 <WS ProdInfo destination info>
 <WS ShipInfo destination info>
 <WS PayInfo destination info>
 <ProdInfo>
  <ProdID>OnlyTheParanoidSurvive</ProdID>
  <Quantity>1</Quantity>
  <Price>34.90</Price>
 </ProdInfo>
 <ShipInfo>
  <Address>2111 NE 25th Avenue</Address>
  <City>Hillsboro</City>
  <State>OR</State>
  <ZIPCode>97124</ZIPCode>
  <Country>USA</Country>
 </ShipInfo>
 <PayInfo>
  <Type>MasterCard</Type>
  <Number>5094289200882312</Number>
  <ExpDate>032007</ExpDate>
 </PayInfo>
</XML>
```

CROWN BOOKS

amazon.com

BARNES&NOBLE BOOKSELLERS

FedEx

```
<XML>
 <PayInfo>
  <Type>MasterCard</Type>
  <Number>5094289200882312</Number>
  <ExpDate>032007</ExpDate>
 </PayInfo>
</XML>
```

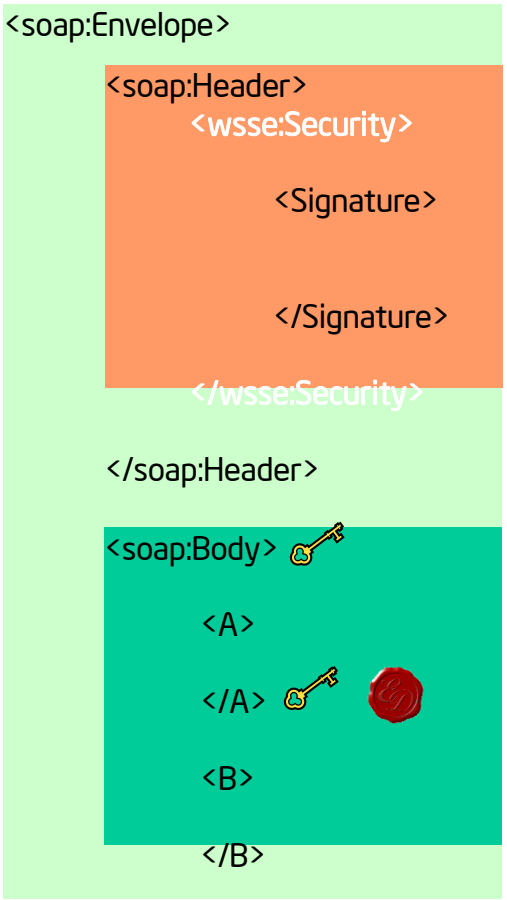
```
<XML>
 <ShipInfo>
  <Address>2111 NE 25th Avenue</Address>
  <City>Hillsboro</City>
  <State>OR</State>
  <ZIPCode>97124</ZIPCode>
  <Country>USA</Country>
 </ShipInfo>
</XML>
```

WS-Security enables content owners to control who has access to it

Content based security is the only solution for securing enterprise integration

WS-Security Anatomy

Secured SOAP Message



Security Feature	Function
SOAP Header	
WS-Security	•Attaches signature, encryption, security tokens to SOAP messages
SAML Token	•Authenticates initiator of SOAP request. •Enables role based authorization. •Time-limited. •Interoperable.
X.509 Certificate	•Encryption and signature verification.
XML Signature, DSIG	•Multiple signed areas of header and body. •Integrity protection via PKI based cryptography. •Prevents tampering.
SOAP Body	
XML Encryption	•Multiple encrypted areas of body. •Prevents disclosure.

A signed SOAP message

WS-Security headers

Signature block

Signed references

Signature value

Signature key

```
<soap:Envelope xmlns:soap="http://...">
    <soap:Header>
        <wsse:Security soap:mustUnderstand="1" xmlns:wsse="http://...">
            <wsse:BinarySecurityToken ValueType="http://..." EncodingType="http://..." wsu:Id=
"FEEE486F-2275-0FD1-4178-E2AAD7575D5E" xmlns:wsu="http://...">(this is the based-64 encoded X509 certificate)
</wsse:BinarySecurityToken>
            <dsig:Signature xmlns:dsig="http://...">
                <dsig:SignedInfo>
                    <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <Reference URI="#WWID34396" xmlns="http://www.w3.org/2000/09/xmldsig#">
                        <Transforms> <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/> </Transforms>
                        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <DigestValue>a01qz2juLu/05YZ11Y11coSGfNo=</DigestValue>
                    </Reference>
                    <Reference URI="#WWID32896" xmlns="http://www.w3.org/2000/09/xmldsig#">
                    <Reference URI="#WWID46464" xmlns="http://www.w3.org/2000/09/xmldsig#">
                    <Reference URI="#7066AFED-7E3D-0E0F-D73D-5AECF77006CC" xmlns="http://www.w3.org/2000/09/xmldsig#">
                </dsig:SignedInfo>
                <dsig:SignatureValue>WfjsiZLiDLaig2Llj.....vvXDZaJtgQ=</dsig:SignatureValue>
                <dsig:KeyInfo>
                    <wsse:SecurityTokenReference> <wsse:Reference URI="#FEEE486F-2275-0FD1-4178-E2AAD7575D5E" ValueType=
"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/> </wsse:SecurityTokenReferenc
                </dsig:KeyInfo>
            </dsig:Signature>
            <wsu:Timestamp wsu:Id="7066AFED-7E3D-0E0F-D73D-5AECF77006CC" xmlns:wsu="http://...">
        </wsse:Security>
    </soap:Header>
    <soap:Body>
        <!-- The goal is to sign only the candidates that will actually be promoted -->
        <promotion_candidates>
            <manager Id="WWID46464">John</manager>
            <engineer Id="WWID34396">Mike</engineer>
            <manager Id="WWID34364">Joe</manager>
            <engineer Id="WWID32896">Tom</engineer>
        </promotion_candidates>
    </soap:Body>
</soap:Envelope>
```

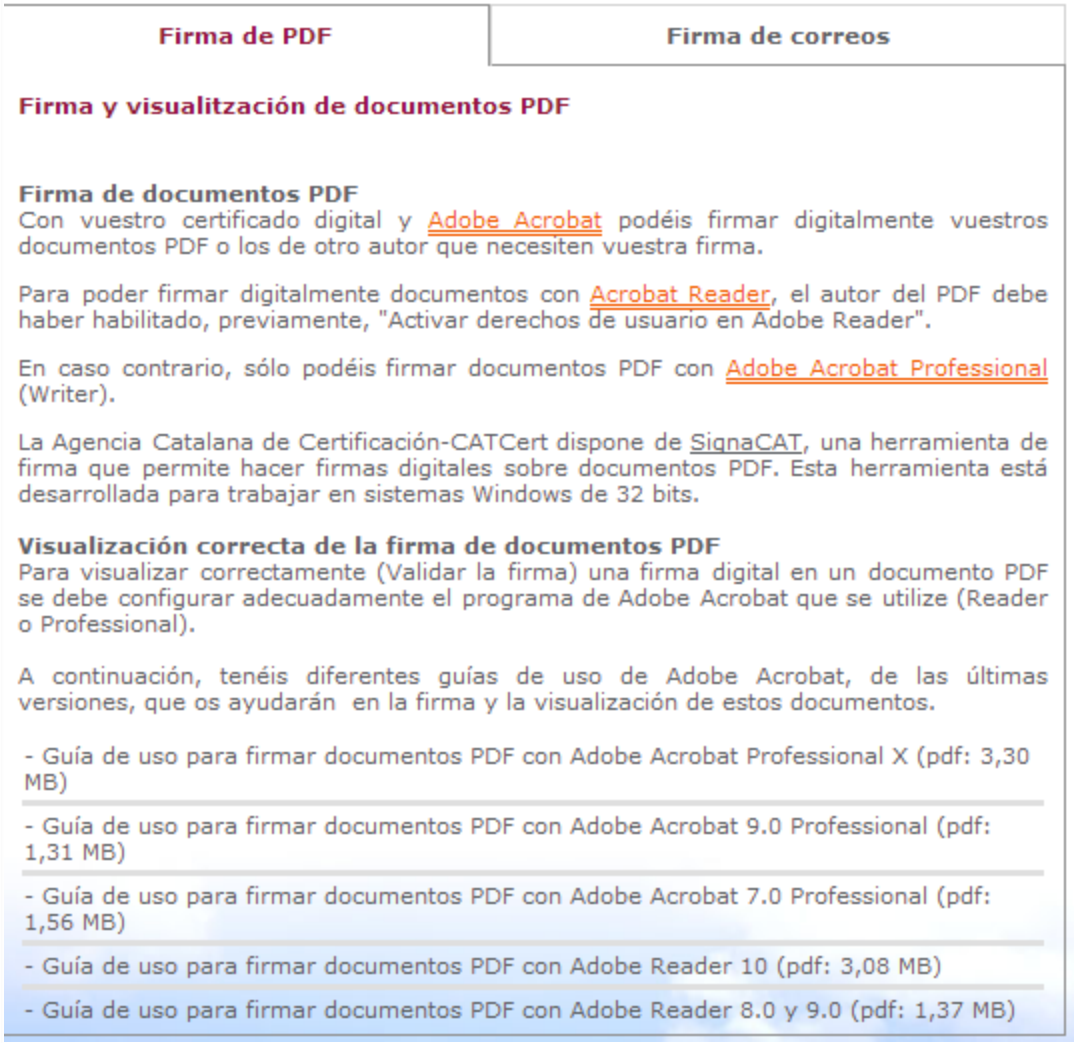
```
<soap:Envelope xmlns:soap="http://..." xmlns:wsu="http://...">
    <soap:Body>
        <!-- The goal is to sign only the candidates that will actually be promoted -->
        <promotion_candidates>
            <manager wsu:Id="WWID46464">John</manager>
            <engineer wsu:Id="WWID34396">Mike</engineer>
            <manager wsu:Id="WWID34364">Joe</manager>
            <engineer wsu:Id="WWID32896">Tom</engineer>
        </promotion_candidates>
```

The content is selectively signed (not the message)

Firma de los documentos mas comunes.
PDF – WORD – EXCEL - PP

http://www.softpedia.es/programa-DigiSigner-162204.html

Firma de los documentos mas comunes. (PDF)



Firma de PDF | Firma de correos

Firma y visualització de documentos PDF

Firma de documentos PDF
Con vuestro certificado digital y Adobe Acrobat podéis firmar digitalmente vuestros documentos PDF o los de otro autor que necesiten vuestra firma.

Para poder firmar digitalmente documentos con Acrobat Reader, el autor del PDF debe haber habilitado, previamente, "Activar derechos de usuario en Adobe Reader".

En caso contrario, sólo podéis firmar documentos PDF con Adobe Acrobat Professional (Writer).

La Agencia Catalana de Certificación-CATCert dispone de SignaCAT, una herramienta de firma que permite hacer firmas digitales sobre documentos PDF. Esta herramienta está desarrollada para trabajar en sistemas Windows de 32 bits.

Visualización correcta de la firma de documentos PDF
Para visualizar correctamente (Validar la firma) una firma digital en un documento PDF se debe configurar adecuadamente el programa de Adobe Acrobat que se utilize (Reader o Professional).

A continuación, tenéis diferentes guías de uso de Adobe Acrobat, de las últimas versiones, que os ayudarán en la firma y la visualización de estos documentos.

- Guía de uso para firmar documentos PDF con Adobe Acrobat Professional X (pdf: 3,30 MB)
- Guía de uso para firmar documentos PDF con Adobe Acrobat 9.0 Professional (pdf: 1,31 MB)
- Guía de uso para firmar documentos PDF con Adobe Acrobat 7.0 Professional (pdf: 1,56 MB)
- Guía de uso para firmar documentos PDF con Adobe Reader 10 (pdf: 3,08 MB)
- Guía de uso para firmar documentos PDF con Adobe Reader 8.0 y 9.0 (pdf: 1,37 MB)

http://www.uab.cat/servlet/Satellite/firma-de-pdf-1266477271311.html

Firma de los documentos mas comunes. (WORD – EXCEL – PP)

cámara Córdoba

PROCEDIMIENTO PARA FIRMAR DIGITALMENTE UN ARCHIVO DE WORD

1. REQUISITOS MÍNIMOS

- Disponer de una versión de Microsoft Word que permita firmar digitalmente los documentos.
- Tener instalado un certificado digital vigente emitido por Camerfirma o por la Fábrica Nacional de Moneda y Timbre (FNMT).

2. PASOS PARA FIRMAR DIGITALMENTE EL ARCHIVO DE WORD.

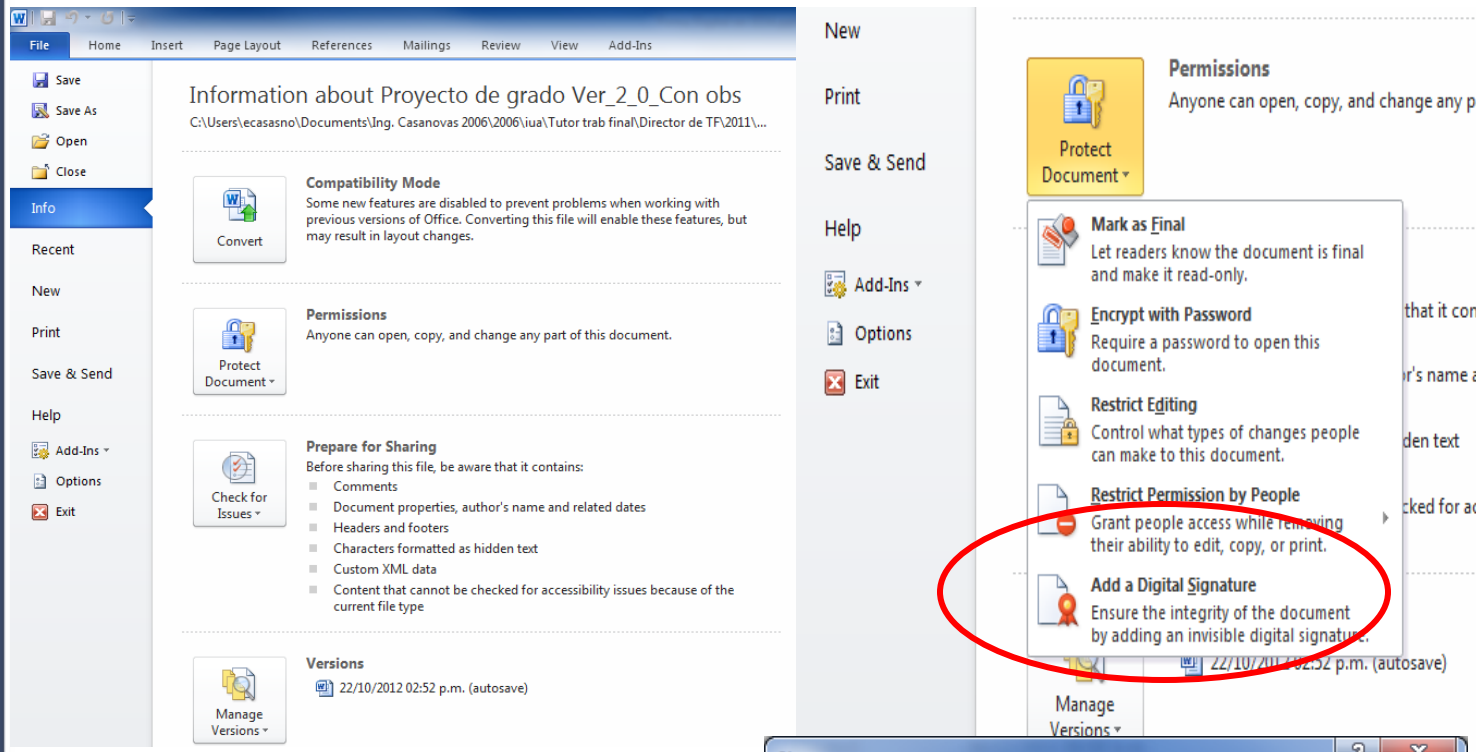
Se recomienda guardar el documento antes de proceder a la firma electrónica del mismo, aunque posteriormente el programa lo solicita en caso de no haberlo hecho.

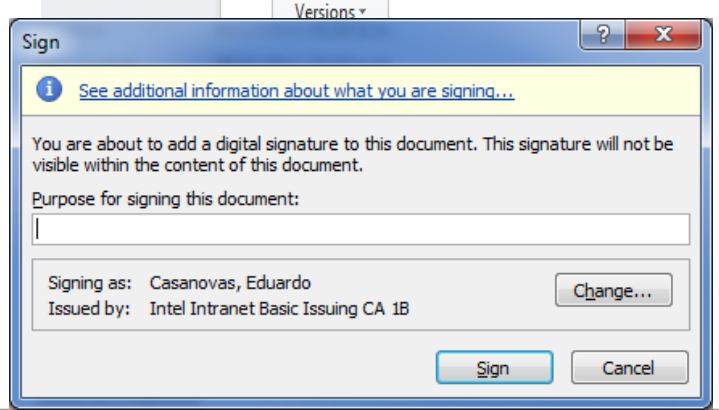
a) En la barra de opciones de Microsoft Word seleccionamos *Herramientas* y dentro del menú que se despliega pulsaremos sobre *Opciones.*

http://www.camaracordoba.com/cordobaexporta/img/imagenes/24_12_05_PROCEDIMIENTO_DE_FIRMA_DIGITAL_DE_ARCHIVOS_WORD._REV.01.pdf

Firmar Digitalmente un documento

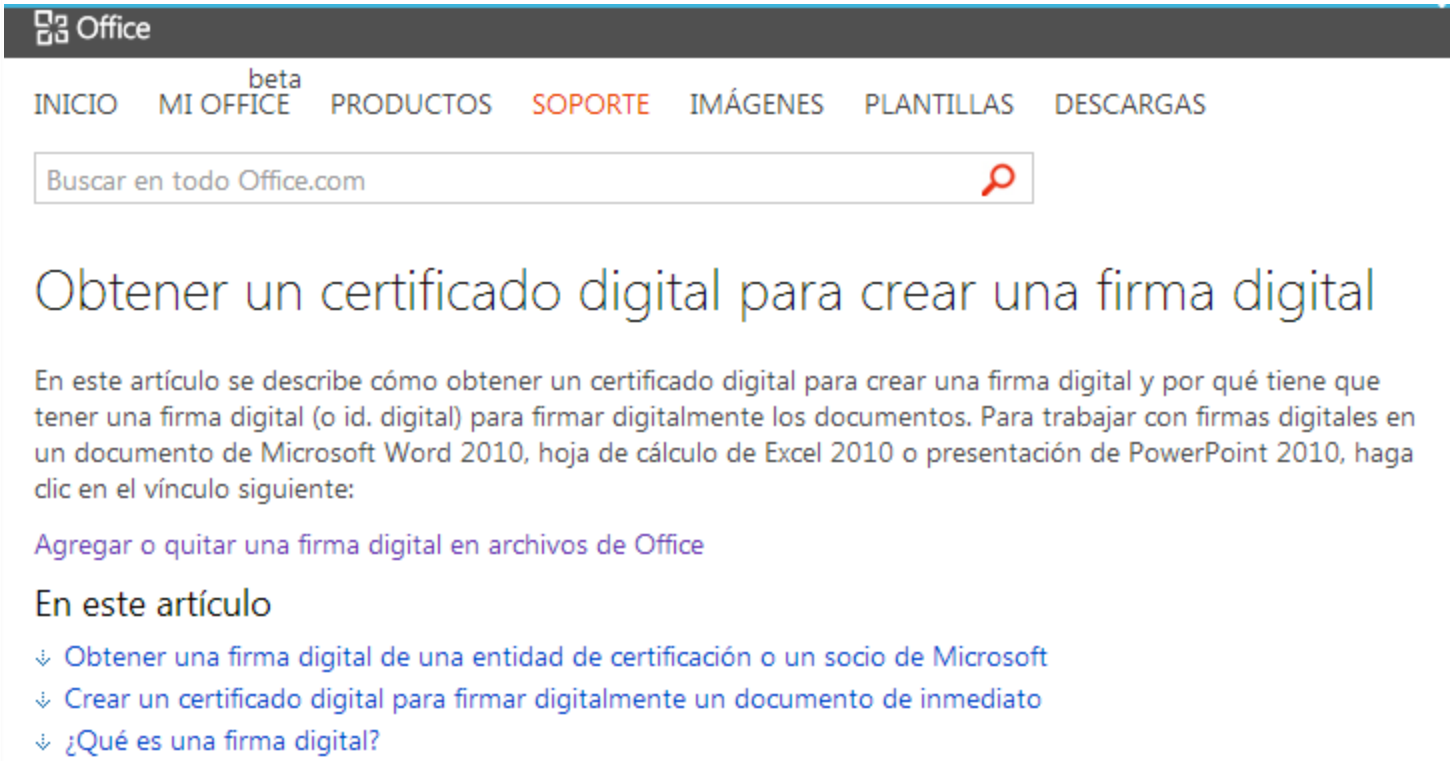
Firma de los documentos mas comunes. (WORD – EXCEL – PP)





Firmar Digitalmente un documento

Firma de los documentos mas comunes. (WORD – EXCEL – PP)



http://office.microsoft.com/es-es/word-help/obtener-un-certificado-digital-para-crear-una-firma-digital-HA010354319.aspx

Firma de los documentos mas comunes. (Outlook)

firmadigital ARGENTINA

Jefatura de Gabinete de Ministros
Presidencia de la Nación

Instructivo de configuración de certificado digital en Outlook Express 6.0

Objetivo: Configurar el cliente de correo Outlook Express versión 6.0 para poder enviar correos electrónicos firmados digitalmente.

Requisitos: Haber instalado con Internet Explorer el certificado digital que se desea utilizar y tener instalada la clave privada correspondiente a ese certificado.

Procedimiento:

1) Acceda al menú [Herramientas] y luego seleccione el ítem [Cuentas...].

http://pki.jgm.gov.ar/docs/Instructivo_para_configuracion_y_firma_de_correo_electronico.pdf

Firma de codigo

Windows | Dev Center - Desktop

Search Dev Center with Bing

Home Dashboard Docs Samples Downloads Support Community

Dev Center - Desktop > Docs > Windows Development Reference > Security and Identity > Cryptography > Cryptography Reference > CryptoAPI Tools Reference > Tools to Sign Files and Check Signatures > SignTool

SignTool

- Learn Windows
- Windows Development Reference
- Security and Identity
- Cryptography
- Cryptography Reference

20 out of 84 rated this helpful - Rate this topic

The SignTool tool is a command-line tool that digitally signs files, verifies signatures in files, or time stamps files. For information about why signing files is important, see Introduction to Code Signing. The tool is installed in the \Bin folder of the Microsoft Windows Software Development Kit (SDK) installation path.

SignTool is available as part of the Windows SDK, which you can download from http://go.microsoft.com/fwlink/?linkid=84091.

Here is the syntax for SignTool:

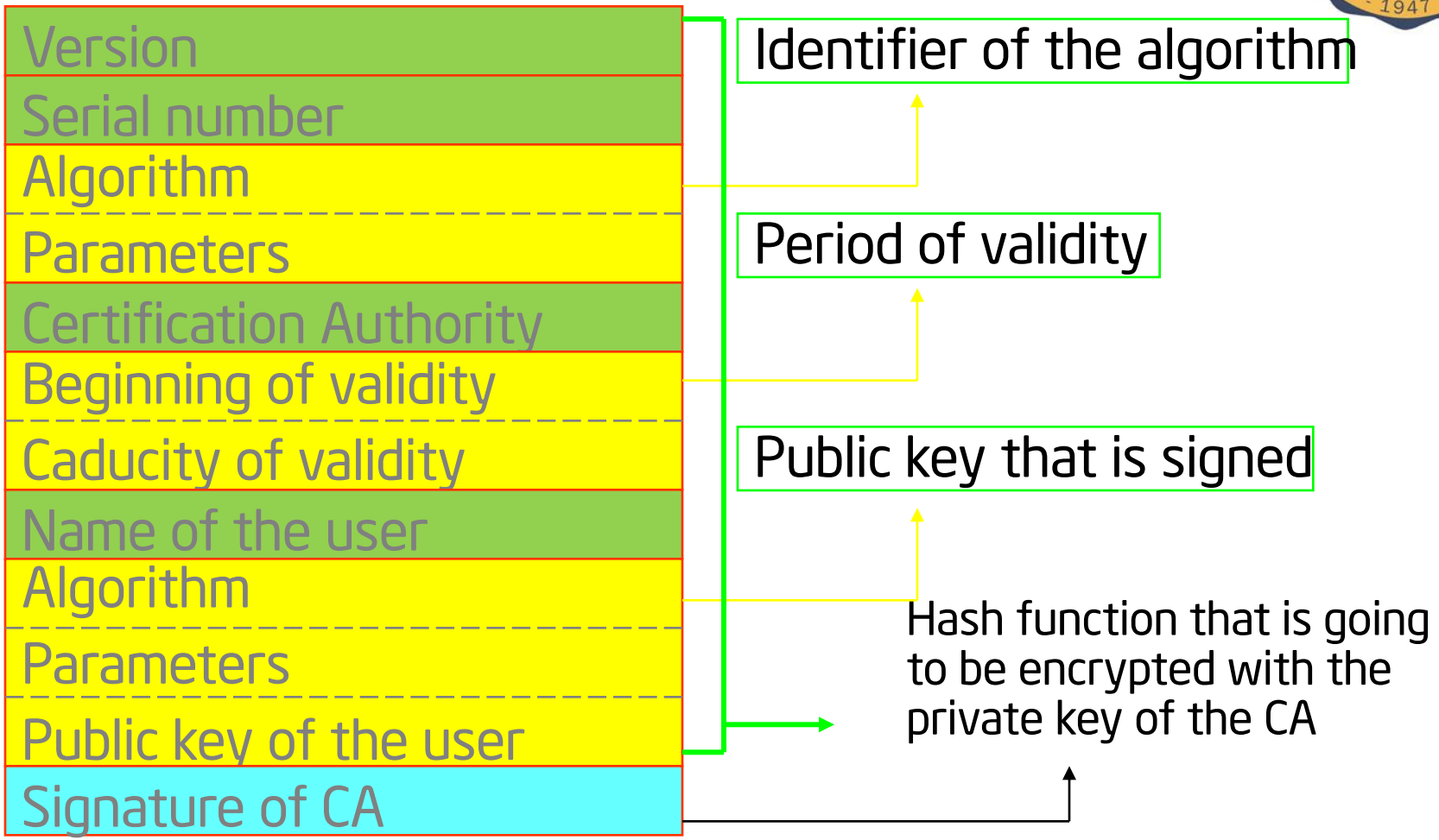
signtool [*Command*][*Options*][*FileName* ...]

The following commands are supported by SignTool.

Command	Description
catdb	Adds or removes a catalog file to or from a catalog database.
sign	Digitally signs files.
signwizard	This command is not supported. **Windows Vista and earlier:** Launches the signing wizard. Only a single file can be specified for the file name command-line parameter.
timestamp	Time stamps files.
verify	Verifies the digital signature of files.

http://msdn.microsoft.com/en-us/library/windows/desktop/aa387764(v=vs.85).aspx

Format of the digital certificate X.509



Ley de Firma Digital 25.506

ARTICULO 2º — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

ARTICULO 5º — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

Q&A

Tks

applause please