Seguridad en la capa de Transporte Vs Seguridad a nivel de Mensaje

Agenda

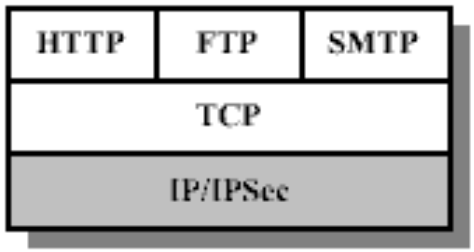
asdc
Argentina Software Development Center

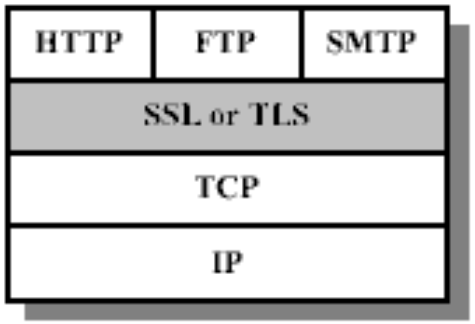
- Sesión SSL
- Frima de un mensaje SOAP
- Proceso de verificación
- Problemas de perfomace
  - Parsing y Canonicalización
  - Forma del mensaje
  - Metricas de complejidad

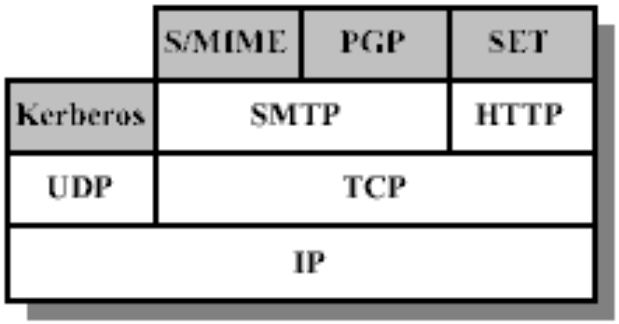
Sesión SSL

asdc
Argentina Software
Development Center

Seguridad en TCP/IP







asdc
Argentina Software Development Center

- Versión actualizada de **SSL** *(Secure Sockets Layer)*
  - ✓ La última versión de SSL (Netscape) fue 3.0
  - ✓ TLS sería SSL v 3.1
  - ✓ Similar, pero no compatible directamente.
  - ✓ Especificado en **RFC 2246** (1999).
- Protege una sesión entre **cliente** y **servidor**.
  - ✓ Típicamente, HTTP (navegador y web server).
- Requiere protocolo de transporte confiable.
  - ✓ Por ejemplo **TCP**.

asdc
Argentina Software Development Center

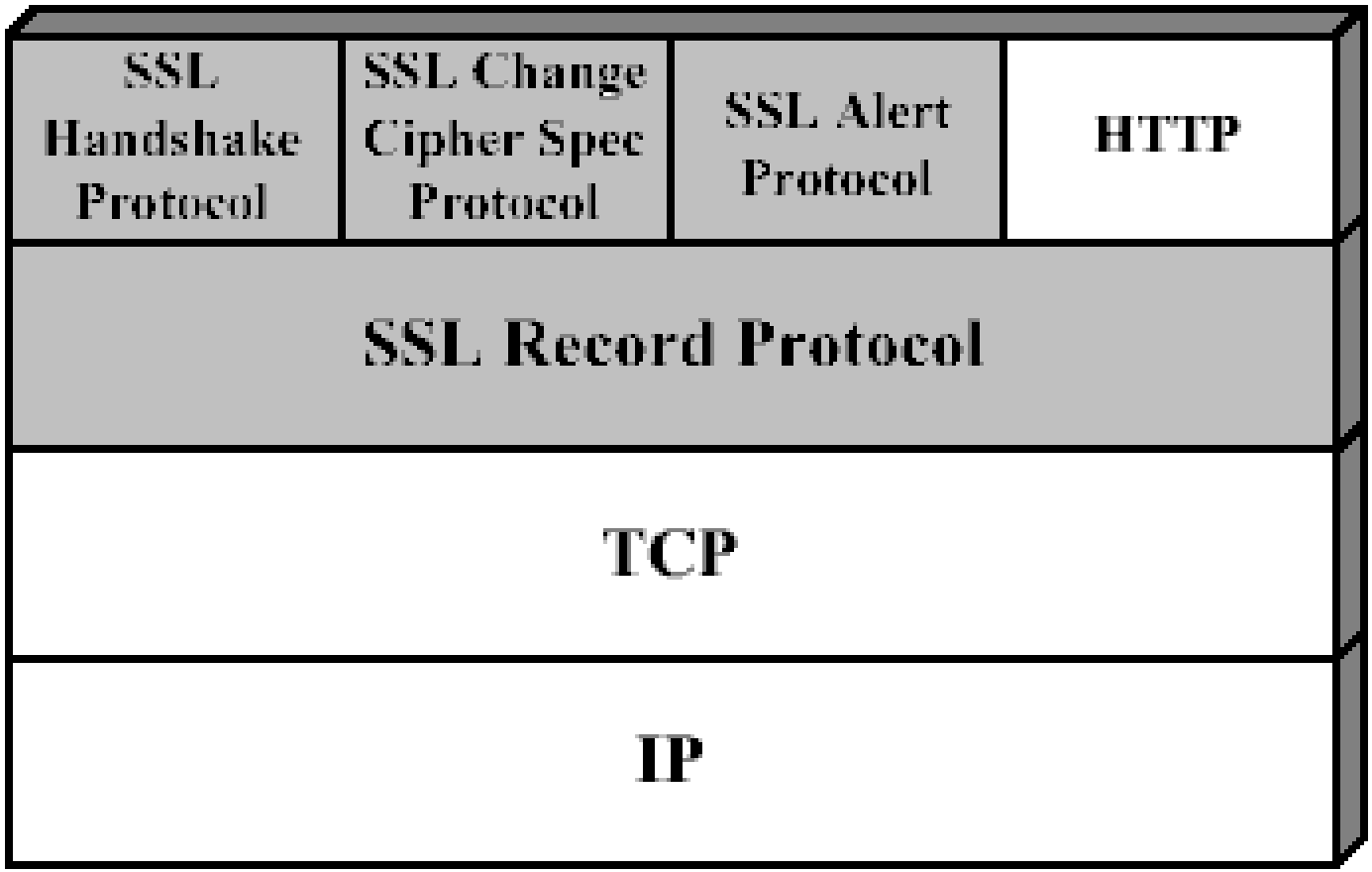
- **Autenticación:**
  - ✓ del servidor frente al cliente;
  - ✓ opcionalmente, del cliente frente al servidor.
  - ⇨ Mediante **certificados** de clave pública.
- **Integridad:**
  - ⇨ Mediante **MAC** y números de secuencia.
- **Confidencialidad:**
  - ✓ opcional.
  - ⇨ Mediante cifrado con algoritmo **simétrico**.

asdc
Argentina Software Development Center

- ***Handshake:***
  - ✓ Negociación de **algoritmos** y parámetros.
  - ✓ **Autenticación** (del servidor o mutua).
  - ✓ Canal seguro para **compartir** un secreto inicial.
  - ✓ Derivación de **claves** en cada extremo.
  - ✓ **Integridad** de todo el intercambio.
- **Transferencia de datos:**
  - ✓ Usa las **claves** anteriormente derivadas.
  - ✓ Provee **integridad**.
  - ✓ Opcionalmente, provee **confidencialidad**.
  - ✓ Autentica el **cierre** de cada conexión.

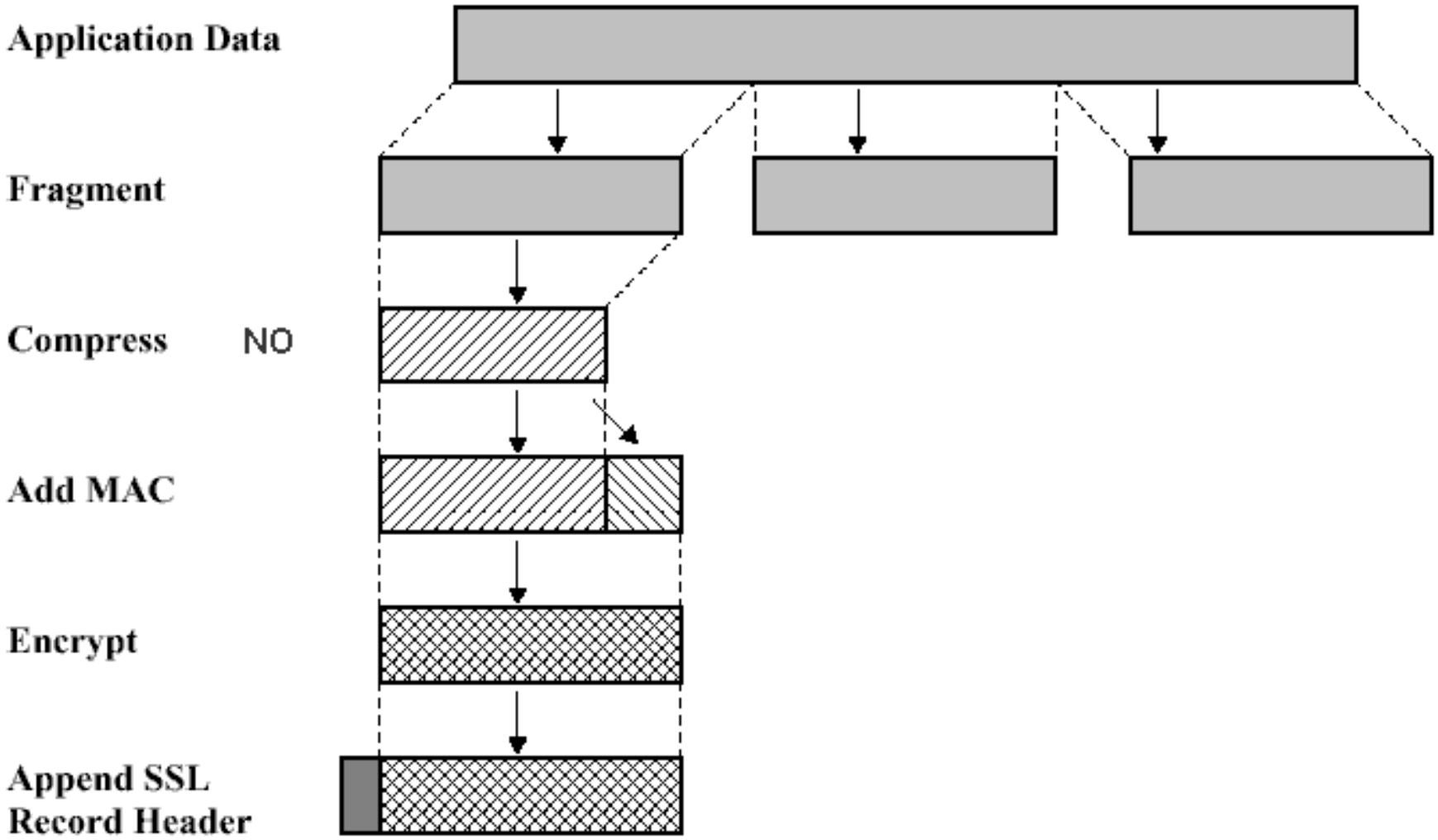
Sesión SSL - Subprotocolos

asdc
Argentina Software Development Center



Sesión SSL - Operación de Record Protocol

asdc
Argentina Software Development Center



Sesión SSL - Alcance de la protección

asdc
Argentina Software Development Center

- El cálculo del MAC abarca:
  - ✓ todos los campos de la **cabecera**,
  - ✓ el **mensaje** útil, y
  - ✓ un **número de secuencia** (8 bytes) que no se transmite: se inicializa en 0 y avanza sincronizada-mente en cliente y en servidor.
    - ⇨ Permite detectar ataques de *replay*, de supresión y de reordenamiento.
- El cifrado para confidencialidad abarca:
  - ✓ el **mensaje** útil, y
  - ✓ el resultado del **MAC**.
    - ⇨ Para cifrado en bloques se agrega suficiente relleno *(padding)* -puede excederse-; el cifrado lo abarca.

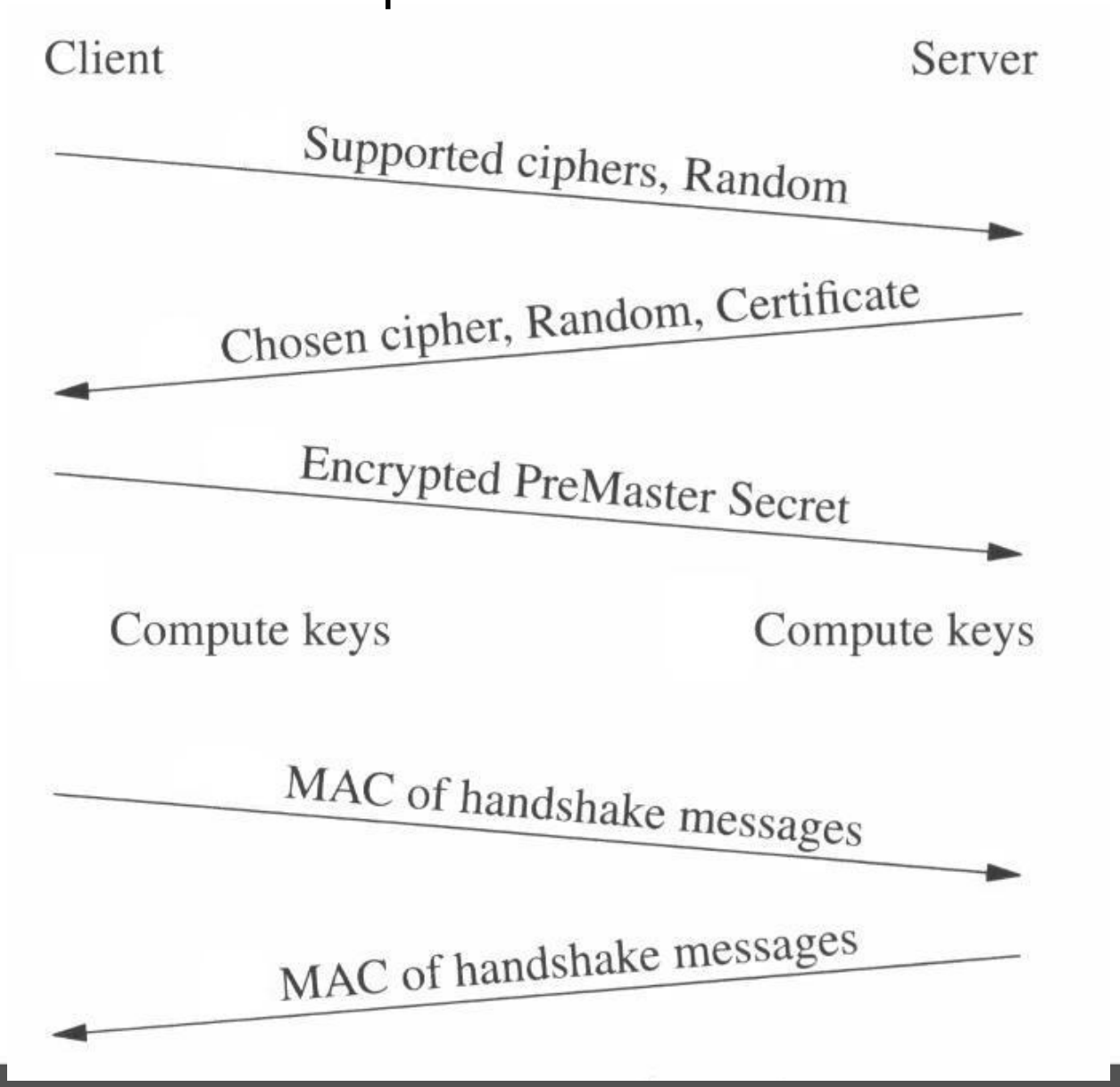
Sesión SSL - Tipo de Msj de HandShake

asdc
Argentina Software Development Center

Message Type	Parameters
hello_request	null
client_hello	version, random, session id, cipher suite, compression method
server_hello	version, random, session id, cipher suite, compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters, signature
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value

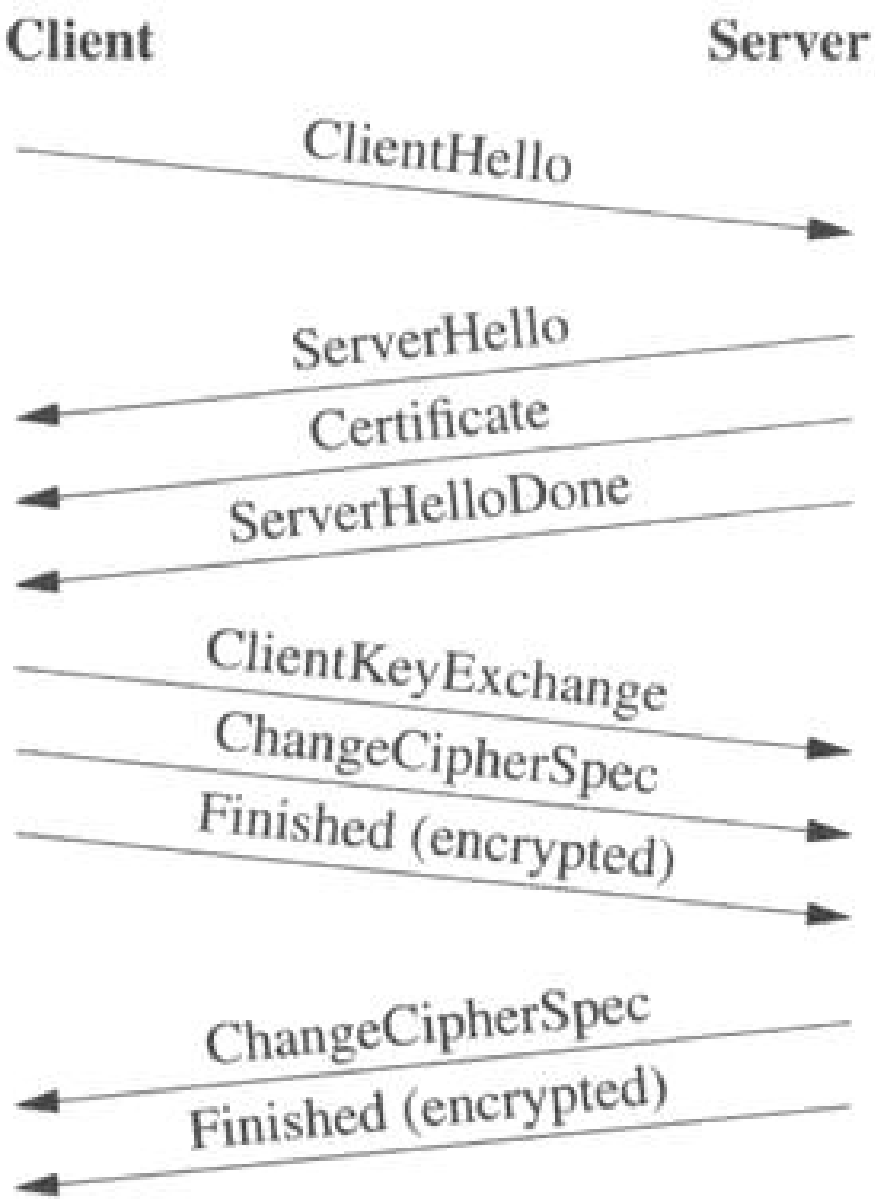
Sesión SSL - Contenido típico del HandShake

asdc
Argentina Software Development Center



Sesión SSL -

HandShake con RSA



Sesión SSL - Conjunto de Algoritmos disponible

asdc
Argentina Software Development Center

Cipher Suite	Auth	Key Exchange	Encryption	Digest	Number
TLS_RSA_WITH_NULL_MD5	RSA	RSA	NULL	MD5	0x0001
TLS_RSA_WITH_NULL_SHA	RSA	RSA	NULL	SHA	0x0002
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA	RSA_EXPORT	RC4_40	MD5	0x0003
TLS_RSA_WITH_RC4_128_MD5	RSA	RSA	RC4_128	MD5	0x0004
TLS_RSA_WITH_RC4_128_SHA	RSA	RSA	RC4_128	SHA	0x0005
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	RSA	RSA_EXPORT	RC2_40_CBC	MD5	0x0006
TLS_RSA_WITH_IDEA_CBC_SHA	RSA	RSA	IDEA_CBC	SHA	0x0007
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	RSA_EXPORT	DES40_CBC	SHA	0x0008
TLS_RSA_WITH_DES_CBC_SHA	RSA	RSA	DES_CBC	SHA	0x0009
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	RSA	3DES_EDE_CBC	SHA	0x000A
TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	RSA	DH_DSS_EXPORT	DES_40_CBC	SHA	0x000B
TLS_DH_DSS_WITH_DES_CBC_SHA	DSS	DH	DES_CBC	SHA	0x000C
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	DSS	DH	3DES_EDE_CBC	SHA	0x000D
TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DH_EXPORT	DES_40_CBC	SHA	0x000E
TLS_DH_RSA_WITH_DES_CBC_SHA	RSA	DH	DES_CBC	SHA	0x000F
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DH	3DES_EDE_CBC	SHA	0x0010

Sesión SSL - Conjunto de Algoritmos disponible

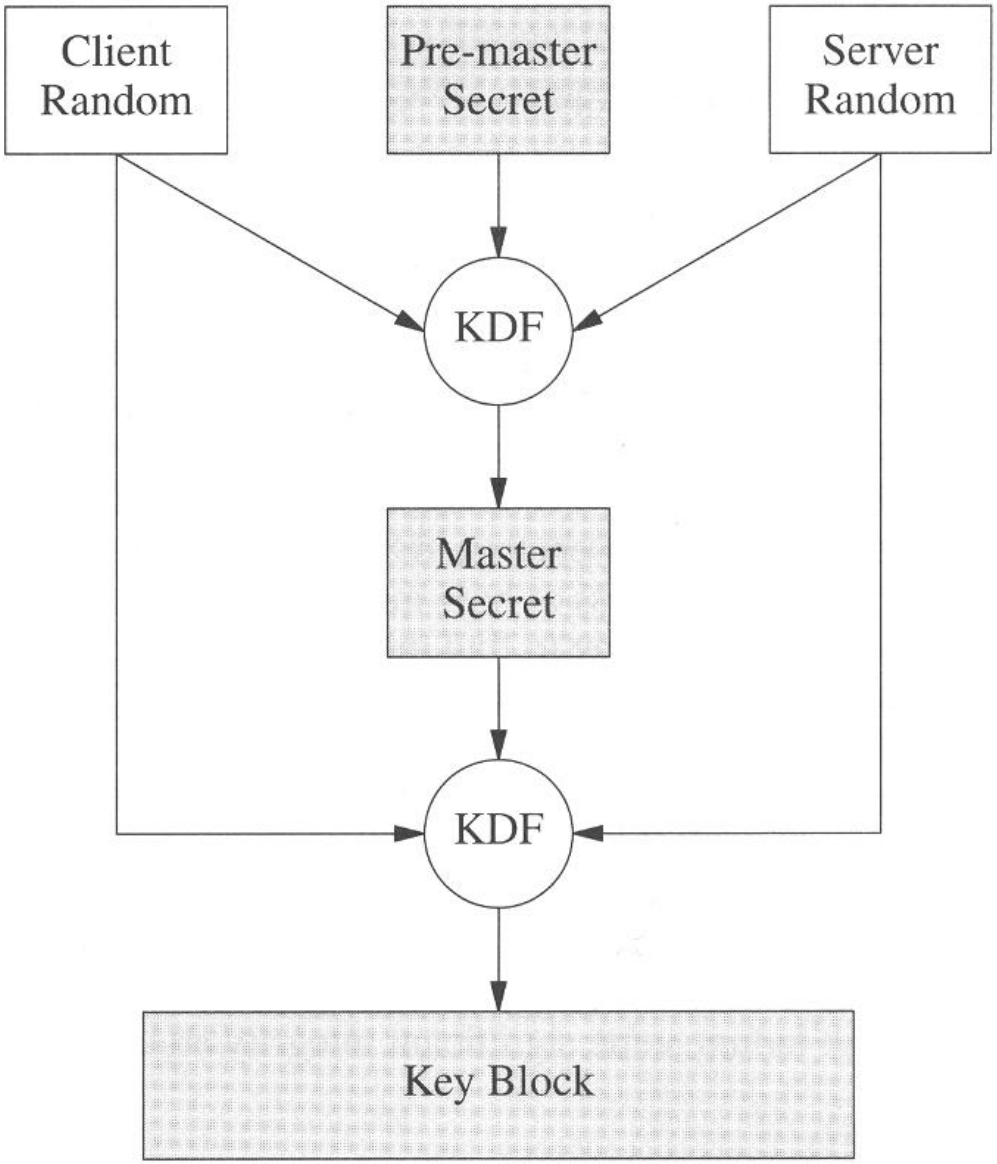
asdc
Argentina Software Development Center

TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	DSS	DHE_EXPORT	DES_40_CBC	SHA	0x0011
TLS_DHE_DSS_WITH_DES_CBC_SHA	DSS	DHE	DES_CBC	SHA	0x0012
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	DSS	DHE	3DES_EDE_CBC	SHA	0x0013
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DHE_EXPORT	DES_40_CBC	SHA	0x0014
TLS_DHE_RSA_WITH_DES_CBC_SHA	RSA	DHE	DES_CBC	SHA	0x0015
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DHE	3DES_EDE_CBC	SHA	0x0016
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	-	DH_EXPORT	RC4_40	MD5	0x0017
TLS_DH_anon_WITH_RC4_128_MD5	-	DH	RC4_128	MD5	0x0018
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	-	DH	DES_40_CBC	SHA	0x0019
TLS_DH_anon_WITH_DES_CBC_SHA	-	DH	DES_CBC	SHA	0x001A
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	-	DH	3DES_EDE_CBC	SHA	0x001B
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA †	RSA	RSA	DES_CBC	SHA	0x0062
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA †	RSA	RSA	DES_CBC	SHA	0x0063
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA †	RSA	RSA	RC4_56	SHA	0x0064
TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA †	RSA	RSA	RC4_56	SHA	0x0065
TLS_DHE_DSS_WITH_RC4_128_SHA †	RSA	RSA	RC4_56	SHA	0x0066

- Por **sesión**: a partir del *pre-master secret* ya comunicado en forma segura, y de los números aleatorios enviados en claro en *ClientHello* y *ServerHello*, cliente y servidor derivan independientemente el *master secret* (48 bytes).
- Por **conexión**: a partir del *master secret* almacenado, y de los nros. aleatorios de esta conexión, ambos extremos derivan independientemente un bloque que luego dividen en:
  - ✓ secretos para el **MAC** de cada uno, y
  - ✓ **claves** de cifrado para cada uno.

Sesión SSL - Generación de Claves

asdc
Argentina Software
Development Center



Porqué hacerlo con SOA,

asdc
Argentina Software Development Center

Porqué con Seguridad?

- **B2B, La integración es una realidad**
  U$s7000B van a ser gastados en transacciones B2B en 2007 (i.e. 45% of the total) (Source IDC)
- **SOA simplifica B2B pero por otro lado se expone a grandes ataques**
  - Compartir APIs permite a los partners y atacantes tener acceso al corazón de nuestras aplicaciones de negocios.
  - Ataque automatizados estan siendo cada vez más frecuentes
    * Web Services Description Language (WSDL)
    * Universal description, discovery, and integration (UDDI)
    * Dejar de lado frente a las pilas de software están en todas partes

  * 75% de los ataque ocurre en el nivel de Application/Servicio (Source Gartner)
- **WS-Security es a SOA como SSL es a HTTP**
  - WS-Security es el único standard para segurizar SOA
    * Grandes vendors estan sopotando SOA(IBM, MS, Verisign)
    * WS-Security se incrementa año a año el número de usuarios

WS-Security apoya a SOA en su crecimiento

- Frima de un mensaje SOAP

asdc
Argentina Software Development Center

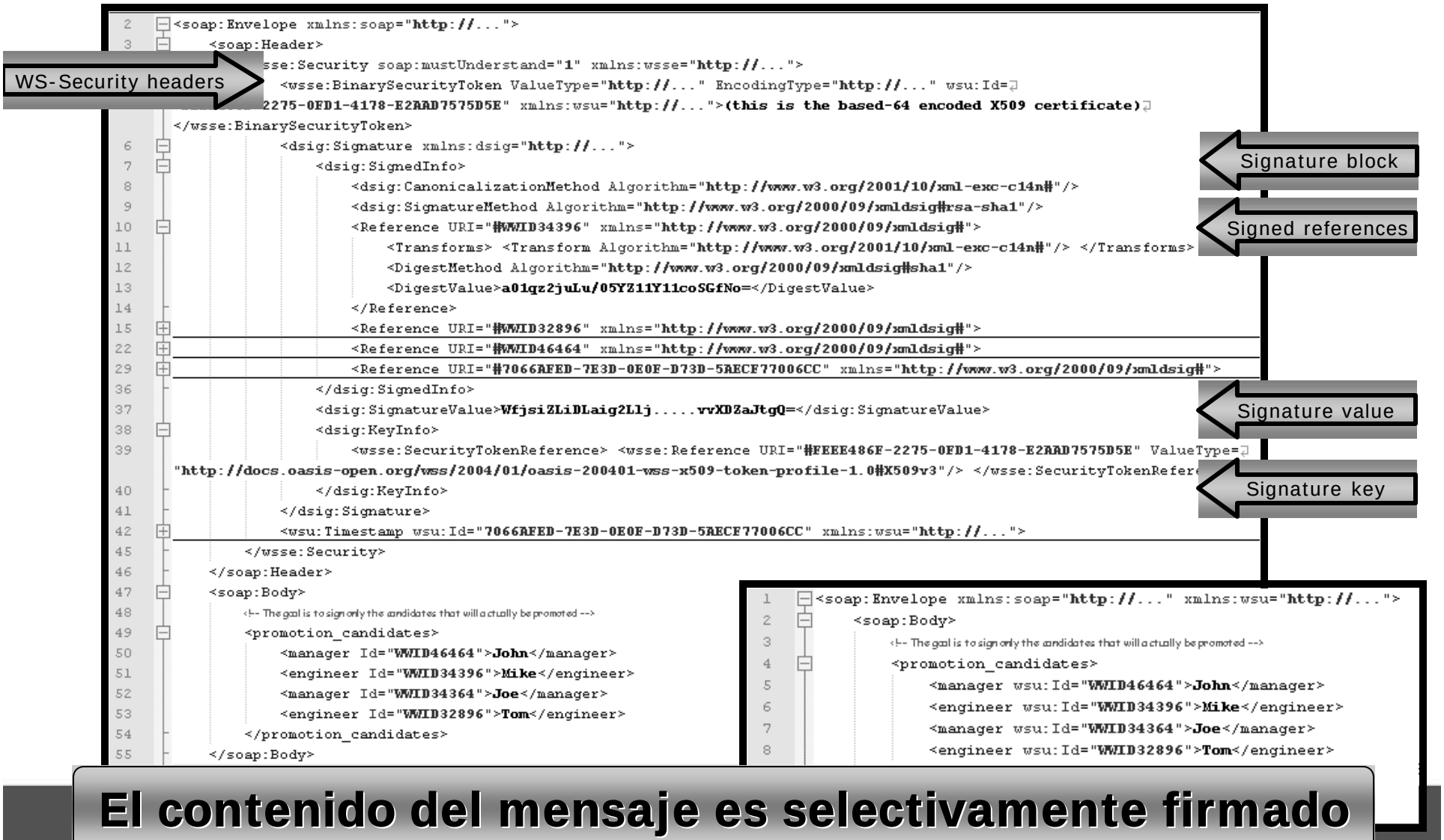
Secured SOAP Message

```
<soap:Envelope>
    <soap:Header>
        <wsse:Security>
            <Signature>
            </Signature>
        </wsse:Security>
    </soap:Header>
    <soap:Body>
        <A>
        </A>
        <B>
        </B>
    </soap:Body>
</soap:Envelope>
```


Author: Eng. Eduardo Casanovas

•Frima de un mensaje SOAP

asdc
Argentina Software Development Center



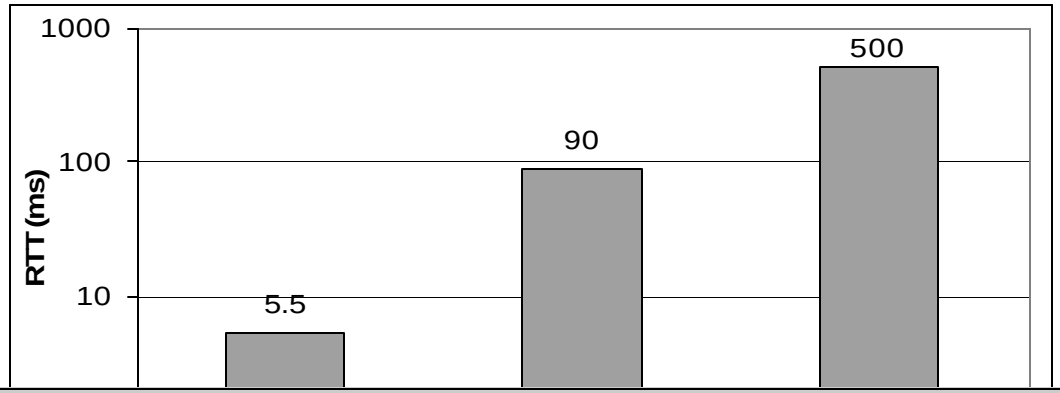
El contenido del mensaje es selectivamente firmado

4. Digital signature applied to XML (1)

Cuanto me cuesta aplicar esto?
SSL vs. WS-Security en Grid Computing

asdc
Argentina Software Development Center

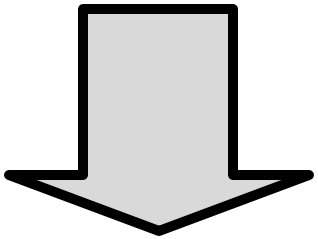
- La prueba (by Shirasuna et.al., 2004)
  - Objetivo: comparar SSL & WS-Security
    - 8 clientes saturan un server con pequeños mensajes (5 bytes payload)
  - Entorno
    - XSUL usando Apache XML Security library (XSUL es más rápido que GT3.2)
    - Tomcat 4.1.30. Sun J2SE 1.4.2_04, Linux 2.4.21
    - Dual Xeon 2.8GHz with 2GB of RAM



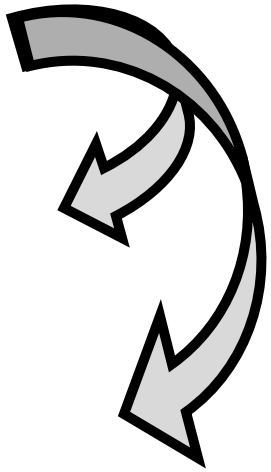
SSL agrega 10X de demora, WS-Security agrega 100X!
(La mayoría de este costo es el procesamiento del xml)

Firma Digital en XML

asdc
Argentina Software Development Center



XML canonicalización (c14n)



Es dificil comparar documentos XML

Dos fragamentos XML pueden tener la misma semántica

<color >blue</color >
Es equivalente a :
<color>blue</color>

applause please

Forma del mensaje

asdc
Argentina Software Development Center

Un caso en el que el documento XML contiene un solo elemento de 1 Mb de texto plano

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP:Envelope xmlns:hl7ebxml="urn:hl7-org:transport/ebxml/DSTUv1.0"
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg.....
   <SOAP:Body>
     <eb:Manifest eb:version="2.0">Reference xlink:href="cid:payload
                @hl7.com location="uniquestuff:PORX_IN020101UK05.xsd"
                eb:version="03" l7ebxml:payload style="HL7" encoding=
                "XML" version="3.0".....
     </eb:Manifest>
   </SOAP:Body>
</SOAP:Envelope>
```

Forma del mensaje

asdc
Argentina Software
Development Center

Es muy diferente de un documento XML con aprox 1000 elementos de Kb cada uno

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP:Envelope xmlns:hl7ebxml="urn:hl7-org:transport/ebxml/DSTUv1.0"
xmlns:eb="http://www.oasis-open.org/committees/ebxml-...../">
      <SOAP:Body>
          <eb:Manifest eb:version="2.0"...../>
          <eb:Reference xlink:href="cid:payload@hl7.com"...../>
          <eb:Schema eb:location="uniquestuff:PORX_IN020...../>
          <eb:Description xml:lang="en-GB">The HL7..</eb:Description>
          .....
          .....
      </SOAP:Body>
</SOAP:Envelope>
```

applause please

Forma del mensaje

asdc
Argentina Software Development Center

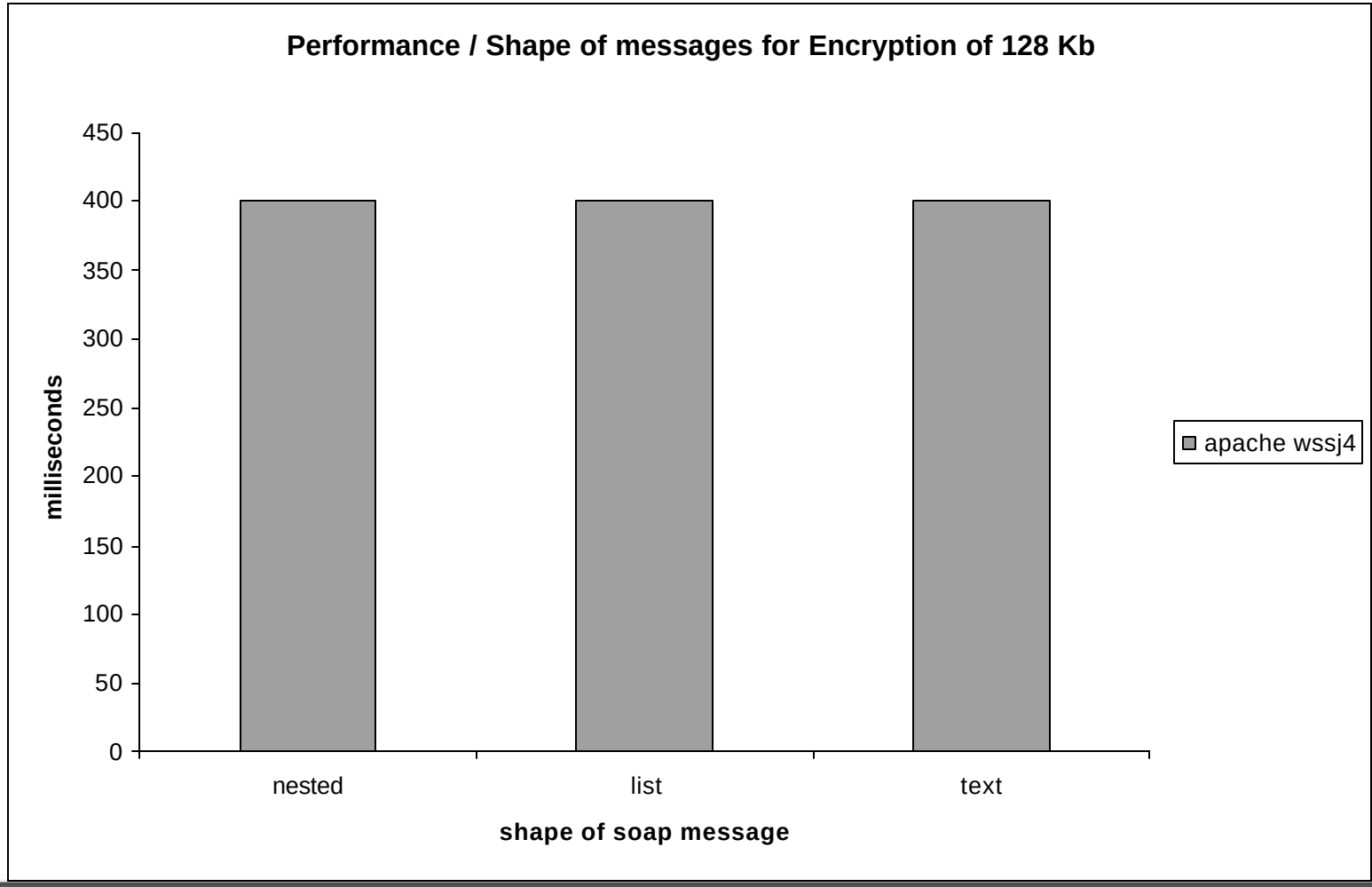
Documento XML con elemntos anidados

```
<?xml version="1.0" encoding="utf-8"?>
<SOAP:Envelope xmlns:hl7ebxml="urn:hl7-org:transport/ebxml/DSTUv1.0"
xmlns:eb="http://www.oasis-open.org/committees/ebxml-...../">
        <SOAP:Body>
            <eb:Manifest eb:version="2.0">
                <eb:Reference xlink:href="cid:payload@hl7.com">
                    <eb:Schema eb:location="uniquestuff:PORX_IN020>
                        <eb:Description xml:lang="en-GB">The HL7>
                                    ..............
                                    ..............
                        </eb:Description>
                    </eb:Schema>
                </eb:Reference>
            </eb:Manifest>
        </SOAP:Body>
</SOAP:Envelope>
```

Métricas

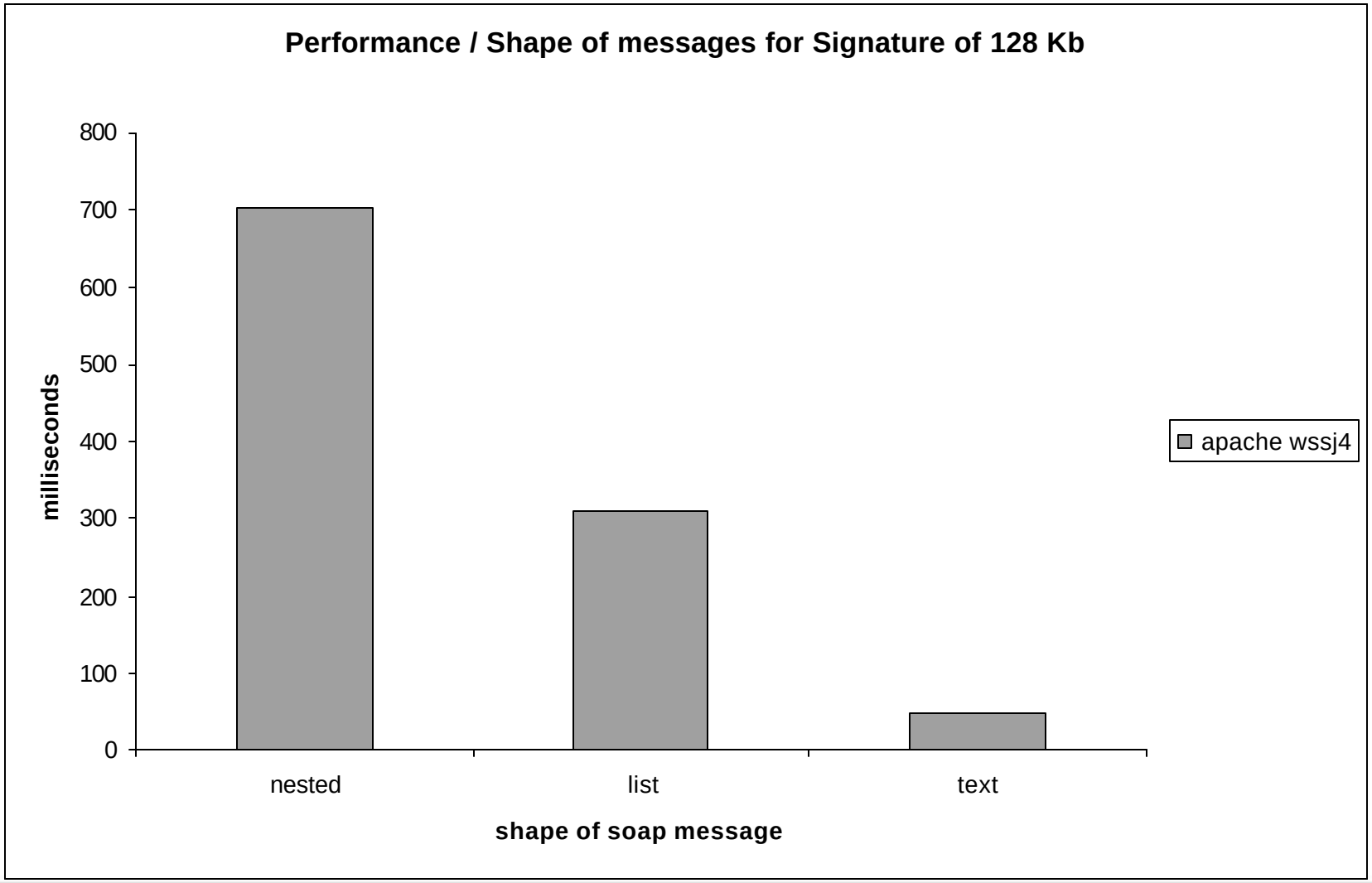
asdc
Argentina Software Development Center

Que sucede si encriptamos...?????



Métricas
Qué sucede si firmamos ...?????

asdc
Argentina Software Development Center



Métricas

XML shape / complexity metric

asdc
Argentina Software Development Center

A los efectos de medir la complejidad de un documento xml, se seleccionó una métrica llamada "iceberg metric", definida de la siguiente forma:

complexity(NodeSet) = sum (nesting(Node) , for each Node in NodeSet) / #NodeSet

nesting(Node) = 1 {si el nodo es un hijo del documento raiz }

nesting(Node) = 1 + nesting(Node.getParentNode()) {Si el nodo no es un hijo del documento raiz }

#NodeSet = Cantidad total de elementos XML (solo XML tags abiertos) in NodeSet

Métricas

asdc
Argentina Software Development Center

```
(1) = <root>
            <nodo_evaluado/>        complejidad es 1 (porque es hijo del nodo raiz)
      </root>


(2) = <root>
            <otro_nodo>
                  <nodo_evaluado/>      complejidad es 2 (1 + nesting(otro_nodo))
            </otro_nodo>
      </root>
```

Métricas
Entorno de prueba

asdc
Argentina Software Development Center

Para el ensayo se utilizó

- Apache's WSS4J 1.5
- Una implementación de WS-Security, con Bouncy Castle como proveedor de seguridad.
- La JVM fue Sun's J2SE 1.6.
- El algoritmo de firma digital seleccionado fue RSA-SHA1.

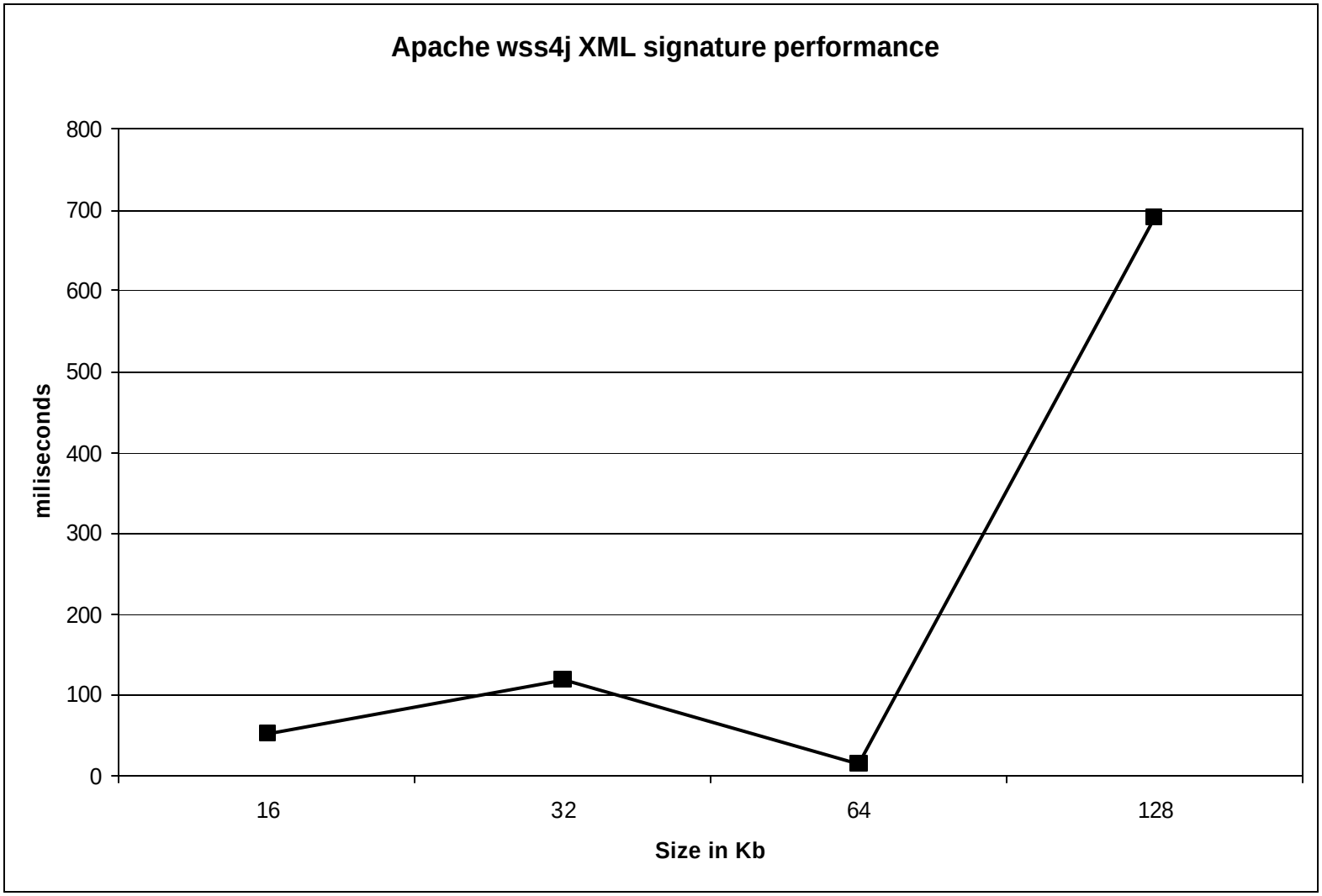
Results

Se firmaron 4 documentos de 16, 32, 64 y 128 Kb respectivamente. Todos ellos con una estructura muy anidada excepto el archivo de 64 Kb que un solo elemento de texto plano.

Métricas

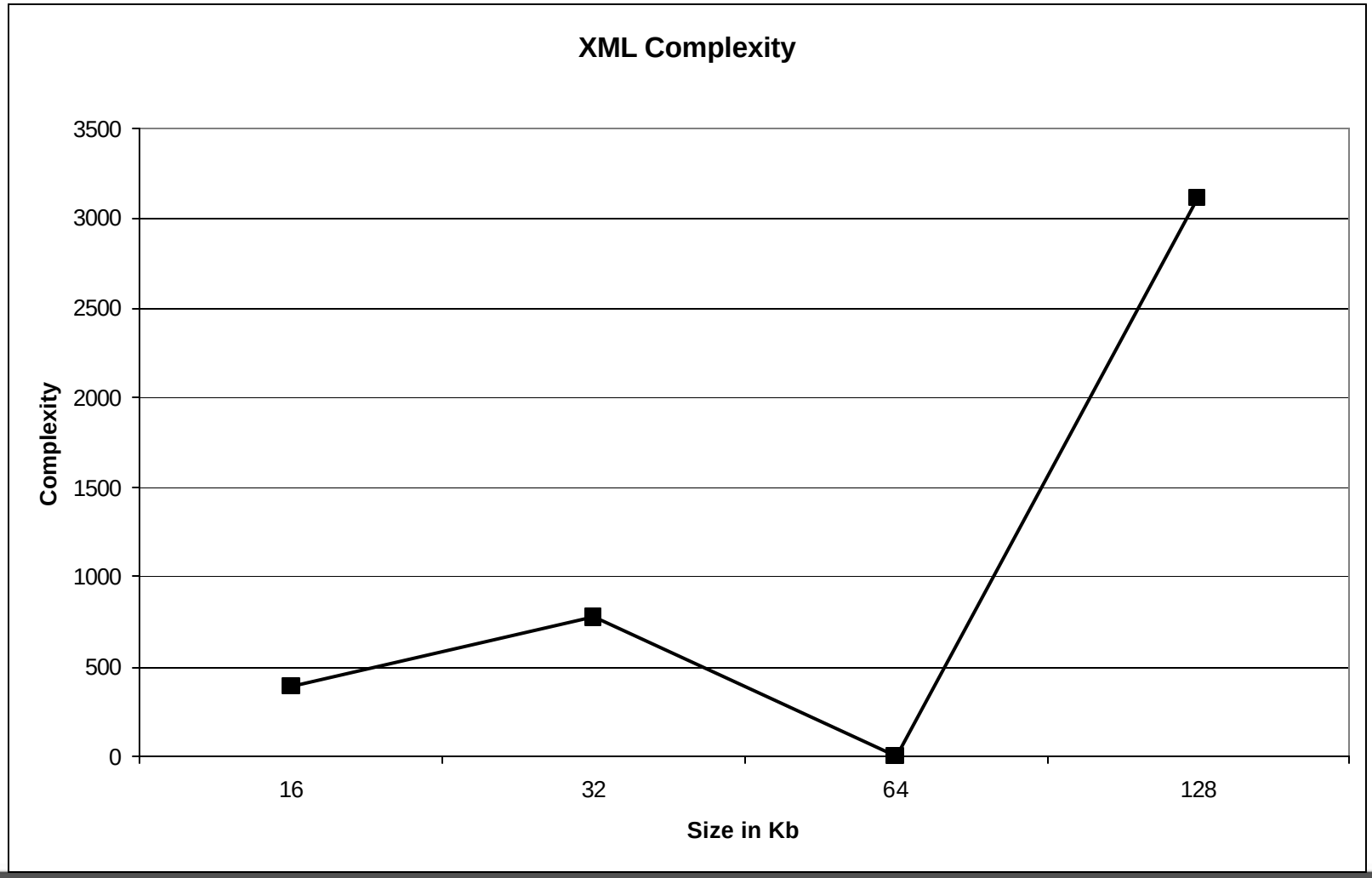
Perfomance del proceso en cada documento

asdc
Argentina Software Development Center



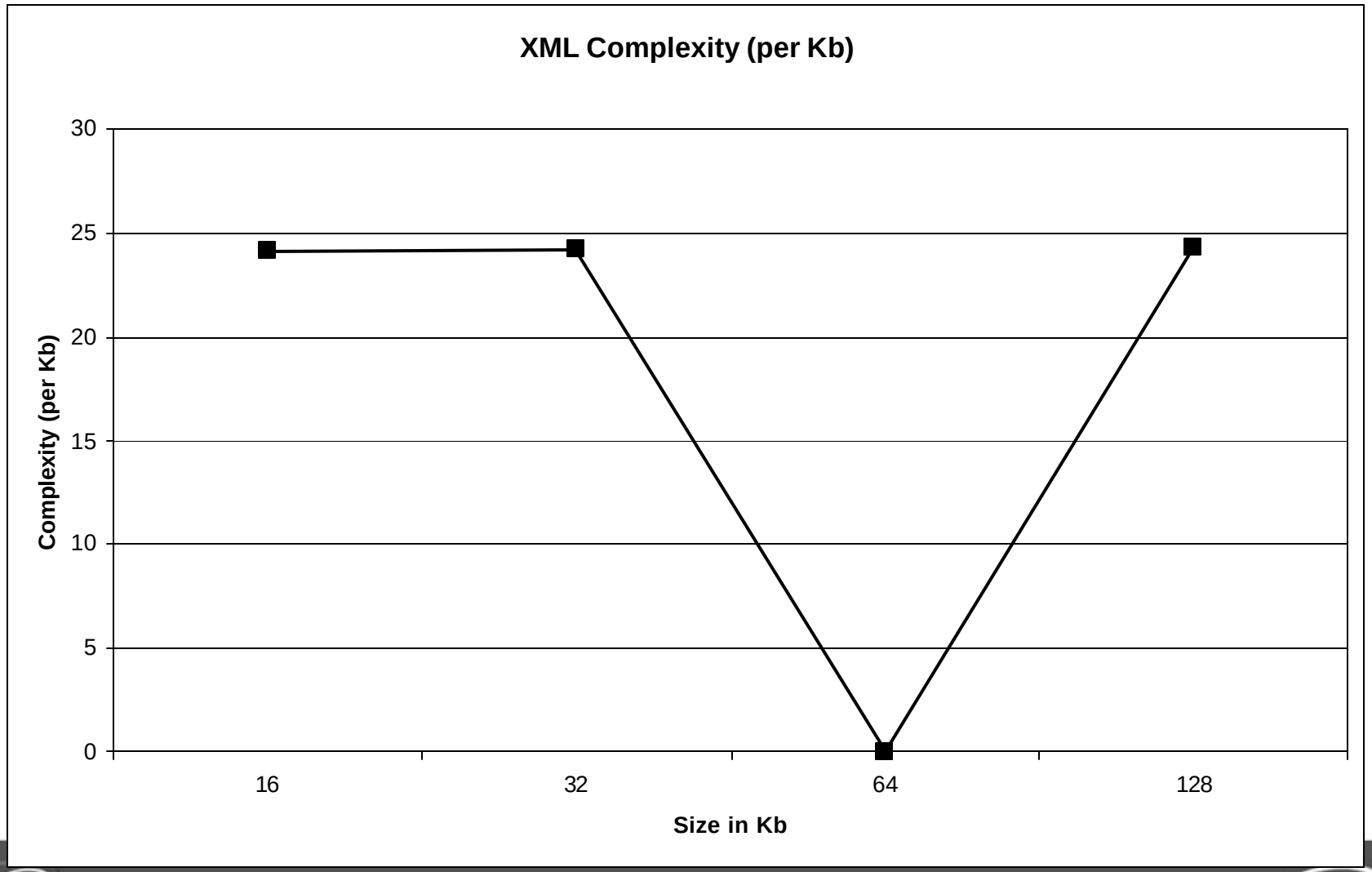
Metricas

La métrica de complejidad por cada documento



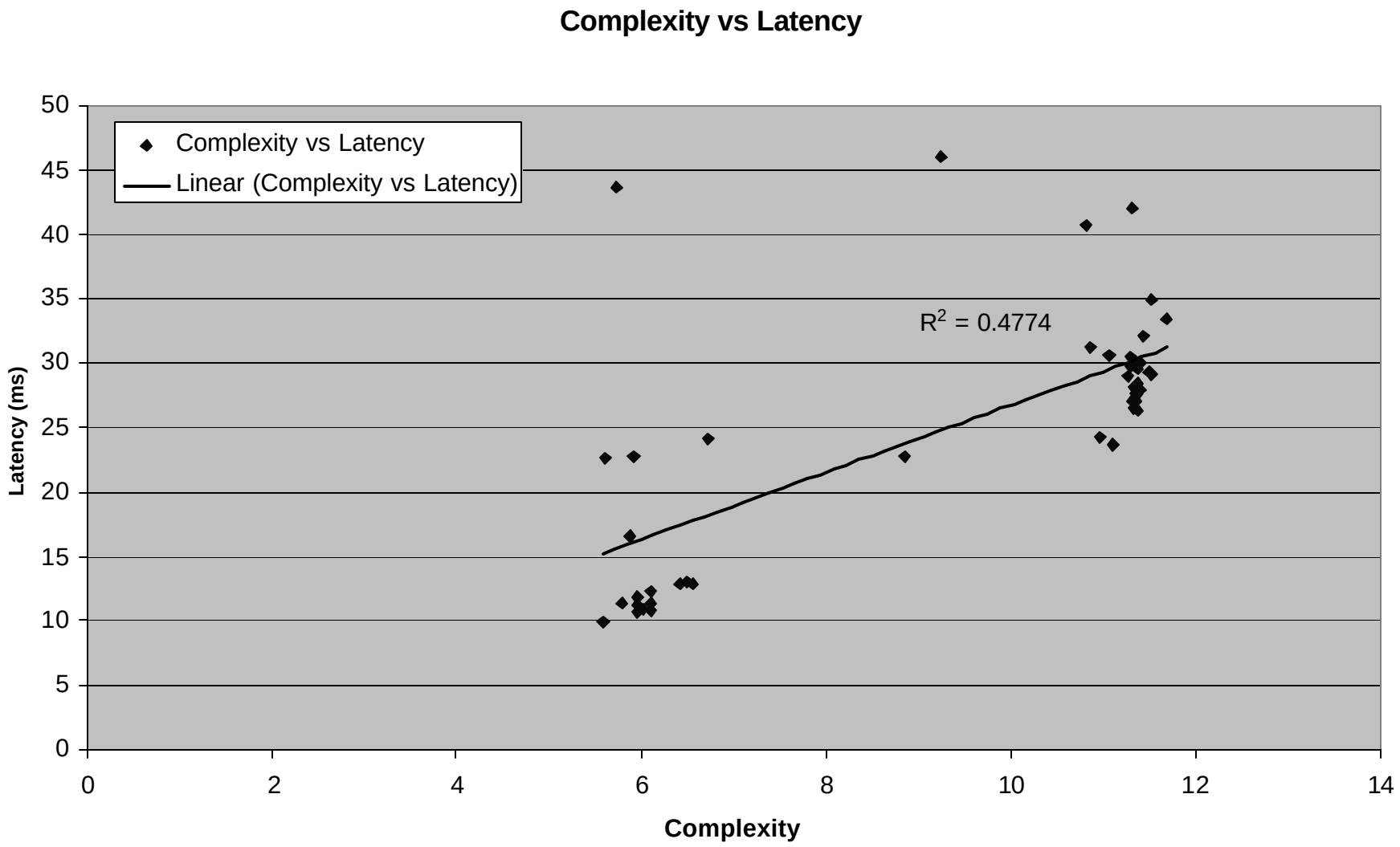
Métricas

Metrica de complejidad normalizada por el tamaño del documento



Métricas

Complejidad vs. Latencia



asdc
Argentina Software Development Center

Q&A

asdc
Argentina Software
Development Center

Tks

applause please