



Università degli studi di Milano
CLS “tecnologie dell’informazione e comunicazione”

Seminario di
Laboratorio di Base di Dati 2

Xml Encryption e Digital Signature

Stefania ACCORDINO 670909
Valeria D’ERRICO 670365




Sicurezza dei dati

Grazie alla sua caratteristiche di flessibilità ed espandibilità, XML è molto utilizzato come formato di scambi dati tra applicazioni.

↓
SVANTAGGIO

Carenza nella protezione dei dati


Accordino e D’Errico 2



Sicurezza dei dati

In molti ambiti (commerciale, militare, etc.) risulta molto importante avere a disposizione uno **strumento in grado di assicurare la protezione dei dati** che vengono scambiati tra le applicazioni.


Accordino e D’Errico 3



SSL (Secure Socket Layer)

- ◆ E’ attualmente lo strumento maggiormente utilizzato per garantire la sicurezza dei dati;
- ◆ permette di creare un canale protetto per lo scambio di dati tra due applicazioni .


Accordino e D’Errico 4



Svantaggio di SSL

- ◆ Non permette di proteggere singole parti del documento, ma per forza tutto il documento intero;
- ◆ Protegge il dato solo durante lo scambio; una volta che esso arriva a destinazione viene decifrato e non è quindi più protetto.


Accordino e D’Errico 5



XML Encryption

- ◆ In XML il problema della sicurezza è affrontato dalla specifica di **XML Encryption**;
- ◆ sviluppato congiuntamente dall'IETF e dal W3C


Accordino e D’Errico 6



XML Encryption

- ◆ E' una tecnologia in grado di proteggere un documento XML o parti di esso;
- ◆ Inoltre è possibile cifrare sia un valore arbitrario (file XML), sia un elemento XML e sia il contenuto di un elemento XML;


Accordino e D'Errico 7



XML Encryption

- ◆ permette di cifrare gli elementi di un documento XML utilizzando i più diffusi algoritmi di crittografia, sia a chiave simmetrica che a chiave pubblica.
- ◆ Il risultato di un dato criptato è un elemento *EncryptedData*

Accordino e D'Errico 8




Struttura

```

<EncryptedData Id? Type??
  <EncryptionMethod/?>
  <ds:KeyInfo>
    <EncryptedKey/?>
    <AgreementMethod/?>
    <ds:KeyName/?>
    <ds:RetrievalMethod/?>
    <ds:*?/?>
  </ds:KeyInfo>
  <CipherData>
    <CipherValue/?>
    <CipherReference URI?/?>
  </CipherData>
  <EncryptionProperties/?>
</EncryptedData>

```

Accordino e D'Errico 9



Struttura


```

<EncryptedData Id? Type??
  <EncryptionMethod/?>
  <ds:KeyInfo>
    <EncryptedKey/?>
    <AgreementMethod/?>
    <ds:KeyName/?>
    <ds:RetrievalMethod/?>
    <ds:*?/?>
  </ds:KeyInfo/?>
  <CipherData>
    <CipherValue/?>
    <CipherReference URI?/?>
  </CipherData>
  <EncryptionProperties/?>
</EncryptedData>

```

Indica l'algoritmo di cifratura utilizzato

Accordino e D'Errico 10



Struttura

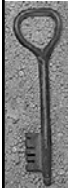
```

<EncryptedData Id? Type??
  <EncryptionMethod/?>
  <ds:KeyInfo>
    <EncryptedKey/?>
    <AgreementMethod/?>
    <ds:KeyName/?>
    <ds:RetrievalMethod/?>
    <ds:*?/?>
  </ds:KeyInfo/?>
  <CipherData>
    <CipherValue/?>
    <CipherReference URI?/?>
  </CipherData>
  <EncryptionProperties/?>
</EncryptedData>

```

Indica la chiave usata per cifrare i dati

Accordino e D'Errico 11



Struttura


```

<EncryptedData Id? Type??
  <EncryptionMethod/?>
  <ds:KeyInfo>
    <EncryptedKey/?>
    <AgreementMethod/?>
    <ds:KeyName/?>
    <ds:RetrievalMethod/?>
    <ds:*?/?>
  </ds:KeyInfo/?>
  <CipherData>
    <CipherValue/?>
    <CipherReference URI?/?>
  </CipherData>
  <EncryptionProperties/?>
</EncryptedData>

```

Contiene i dati cifrati o un riferimento alla loro posizione

Accordino e D'Errico 12



Struttura


```

<EncryptedData Id? Type?>
  <EncryptionMethod/?>
  <ds:KeyInfo>
    <EncryptedKey/?>
    <AgreementMethod/?>
    <ds:KeyName?>
    <ds:RetrievalMethod?>
    <ds:*?>
  </ds:KeyInfo?>
  <CipherData>
    <CipherValue?>
    <CipherReference URI?/?>
  </CipherData>
  <EncryptionProperties?/?>
</EncryptedData>

```

Fornisce altre informazioni sulla generazione dei dati cifrati

Accordino e D'Errico 13




Esempio 1/3

```

<?xml version="1.0"?>
<acquirente>
  <nome>Mario Rossi</nome>
  <carta_di_credito>
    <numero>1234 5678 9123
    4567</numero>
    <scadenza>12/2003</scadenza>
  </carta_di_credito>
</acquirente>

```

Accordino e D'Errico 14



Esempio 2/3

```

<?xml version="1.0"?>
<acquirente>
  <nome>Mario Rossi</nome>
  <carta_di_credito>
    <EncryptedData Id="Enc_esempio"
      Type="http://www.w3.org/2001/04/xmlenc#Element"
      xmlns="http://www.w3.org/2001/04/xmlenc#"
      <EncryptionMethod
        Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
        1_5"/>


```

Contiene i dati protetti e le informazioni sull'algoritmo utilizzato

Tipo di algoritmo usato per decifrare

L'attributo type permette di capire quali elementi decifrare

Accordino e D'Errico 15



Esempio 3/3

```


<ds:KeyInfo
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:KeyName>M_Rossi</ds:KeyName>
  <ds:KeyInfo>
    <CipherData>
      <CipherValue>A55BDBC11</CipherValue>
    </CipherData>
  </ds:KeyInfo>
  <EncryptedData>
    <scadenza>12/2003</scadenza>
  </EncryptedData>
  <carta_di_credito>
    <numero>1234 5678 9123
    4567</numero>
  </carta_di_credito>
</ds:KeyInfo>

```

Contiene le informazioni sulla chiave da utilizzare

racchiude i dati codificati


Accordino e D'Errico 16



Vantaggi

- Questo standard cripta anche le informazioni appartenenti al dato da proteggere (es. cripta "n_carta")
- Visto che è difficile inserire in un documento XML un dato binario, il sistema trasformerà il dato utilizzando un algoritmo Base64

Accordino e D'Errico 17



Seminario di laboratorio di db2: Encryption e Digital Signature

Autenticazione del documento.

XML Digital Signature

Accordino e D'Errico 18

introduzione

- ◆ La sicurezza dei dati è correlata al problema dell'**autenticazione** e dell'**integrità** dei documenti, oltre alla segretezza.
- ◆ Per l'autenticazione di un documento si ricorre alla tecnica della digital signature.
- ◆ La firma si ottiene usando un **algoritmo di cifratura a chiave pubblica**.

Hash di un documento

- ◆ Non si cifra il documento, ma il suo digest, detto anche hash.
- ◆ La funzione hash è molto sensibile ad ogni cambiamento del documento e quindi differenti versioni produrranno digest diversi.
- ◆ Il digest è usato per verificare l'integrità del documento.

Xml signature

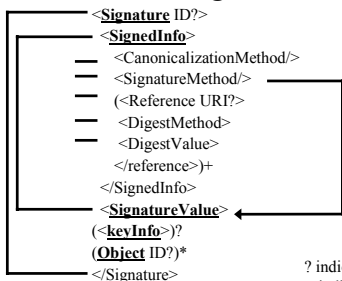
- ◆ Tutti questi aspetti vengono considerati nello standard **XML DIGITAL SIGNATURE**. (IETF e W3C)
- ◆ Si tratta di una tecnologia che permette di cifrare i documenti xml, o parte di essi, garantendone autenticità e integrità.

Xml signature

- ◆ Il processo di validazione prevede 2 passi:
 - 1) Si valida la firma stessa, associando al soggetto che si vuole firmare l'integrità del valore digest dell'elemento firmato, che viene inserito, insieme ad altri valori, in un elemento XML.
 - 2) Infine viene generato un digest. Dopo si valida il valore digest di ciascun dell'elemento che viene firmato con chiave privata.

Struttura generica dell'elemento

<Signature>



? indica 0 o 1 occorrenza,
+ indica 1 o + occorrenze
* indica 0 o + occorrenze

Esempio/1 con Digital Signature

```

<?xml version="1.0" ?>
<signature xmlns=
  http://www.w3.org/2000/09/xmldsig# >
  (1)<SignedInfo Id="esempio_firma">
  <CanonicalizationMethod
    Algorithm=
  http://www.w3.org/TR/2001/REC-xml-c14n-
  20010315/>
    
```

Esempio/2 con Digital Signature

```
<SignatureMethod Algorithm=
  http://www.w3.org/2000/097xmldsig#dsa-sha1/>
<Reference
  URI="http://nome_dominio/eseempio.xml#acq">
<DigestMethod Algorithm=
  http://www.w3.org/2000/09/xmldsig#sha1"/>
```

Esempio/3 con Digital Signature

```
<DigestValue>
  J4fdsu4325riwjerfow732ewjdp9
</DigestValue>
</Reference>
</SignedInfo>
(2)<SignatureValue>
  ME4324W
</SignatureValue>
```

Esempio/4 con Digital Signature

```
(3)<KeyInfo>
  <DSAKeyValue>
    ....
  </DSAKeyValue>
</KeyInfo>
</Signature>
```

<Transform>

- ◆ In alcuni casi il verificatore della firma deve effettuare delle trasformazioni prima di poter correttamente controllare la firma.
- ◆ Le trasformazioni si definiscono con l'elemento <transform> e sono incluse all'interno dell'elemento <reference>.

<Transform>

- ◆ Indica il tipo di trasformazione da effettuare e l'elemento su cui effettuarlo, contenuto in <data reference>

<Transform>

```
<Signature ID?>
<SignedInfo>
  <CanonicalizationMethod/>
  <SignatureMethod/>
  (<Reference URI?>
    (<Transform>
      <data reference>
        </transform?>)
    <DigestMethod/>
    <DigestValue>
  </reference?>+
</SignedInfo>
<SignatureValue>
  (<keyInfo?>)?
  (Object ID)?*
</Signature>
```

<Transform>

- ◆ Il verificatore della firma deve effettuare 2 trasformazioni prima di poterla controllare:
 - 1) la prima per decifrare l'elemento contenuto in data reference;
 - 2) la seconda per scrivere l'elemento in forma canonica.



Fine
xml encryption e
digital signature

