

XML w bazach danych i bezpieczeństwie

Patryk Czarnik

Instytut Informatyki UW

XML i nowoczesne technologie zarządzania treścią – 2007/08

Plan

- 1 Bazy danych
 - XML w relacyjnych bazach danych
 - XML-owe bazy danych

- 2 XML w bezpieczeństwie
 - XML Signature
 - XML Encryption

Klasyfikacja wsparcia dla XML-a w bazach danych

- (Relacyjna) baza danych ze wsparciem dla XML:
 - konfiguracja struktur danych przy pomocy tabel i relacji,
 - eksport i import danych w postaci dokumentów XML,
 - struktura dokumentów XML pochodną relacyjnych struktur danych,
 - zastosowanie: integracja, wymiana danych;
- XML-owa baza danych:
 - przechowuje dokumenty XML,
 - konfiguracja struktur danych przy pomocy DTD/XML Schema,
 - indeksowanie elementów, atrybutów, wyrażeń XPath,
 - wyszukiwanie z użyciem XQuery,
 - zastosowanie: przechowywanie i przetwarzanie dokumentów strukturalnych.

Klasyfikacja wsparcia dla XML-a w bazach danych

- (Relacyjna) baza danych ze wsparciem dla XML:
 - konfiguracja struktur danych przy pomocy tabel i relacji,
 - eksport i import danych w postaci dokumentów XML,
 - struktura dokumentów XML pochodną relacyjnych struktur danych,
 - zastosowanie: integracja, wymiana danych;
- XML-owa baza danych:
 - przechowuje dokumenty XML,
 - konfiguracja struktur danych przy pomocy DTD/XML Schema,
 - indeksowanie elementów, atrybutów, wyrażeń XPath,
 - wyszukiwanie z użyciem XQuery,
 - zastosowanie: przechowywanie i przetwarzanie dokumentów strukturalnych.

XML w relacyjnych bazy danych

- Korzyści:
 - integracja aplikacji, wymiana danych,
 - łatwe transformacje danych,
 - prezentacja danych.
- Problemy:
 - czy i jak przechowywać dokumenty XML w bazie danych?
 - metody dostępu (zadawania zapytań),
 - efektywność.

XML a relacyjne bazy danych

- Przechowywanie XML-a w relacyjnych bazach danych:
 - elementy dokumentu XML jako pola tabeli bazodanowej (dokument „rozłożony na czynniki pierwsze”),
 - dokument XML w całości przechowywany w polu bazy danych.
- Sposoby wspierania XML-a przez systemy zarządzania bazami danych:
 - generowanie XML-a na podstawie zawartości bazy danych,
 - wypełnianie zawartości bazy na podstawie zawartości dokumentu XML,
 - specjalne indeksowanie pól zawierających XML,
 - wbudowane parsery XML i procesory XSLT,
 - integracja z serwerem WWW.

XML w Oracle

- Wsparcie dla XML w Oracle 10g (<http://www.oracle.com/xml>).
- Parsery XML dostarczane przez Oracle:
 - pozwalają na wykorzystanie XML-a we własnych aplikacjach korzystających z bazy,
 - dostępne dla PL-SQL-a, Javy i C++.
- XML-SQL Utility:
 - generowanie XML-a bezpośrednio z bazy przy pomocy specjalnych zapytań,
 - wypełnianie bazy na podstawie zawartości dokumentu XML.
- Typ danych XMLType.

XML w Oracle – XML-SQL Utility

Eksport XML – funkcja `getXML()`

```
SELECT xmlgen.getXML('select * from emp') FROM dual;
```

```
<rowset>
  <row id="1">
    <empno>10</empno>
    <name>Scott Tiger</name>
    <title>specialist</title>
  </row>
  ...
</rowset>
```

XML w Oracle

- `XMLType` – specjalny typ danych:
 - kolumny, tabele, perspektywy, zmienne, ...
 - indeksowanie zawartości XML,
 - zapytania XQuery,
 - kontrola poprawności strukturalnej względem XML Schema,
 - przekształcenia XSLT.
- Specjalne operatory:
 - `extract`, `extractValue`, `existsNode`, `transform`, `updateXML`, `XMLSequence`.
- XPath Rewrite –przekształcanie ścieżek XPath w równoważne konstrukcje SQL na wewnętrznej reprezentacji strukturalnej `XMLType`.

Tamino – XML-owa baza danych

- Pierwszy serwer „bazodanowy” przechowujący dane w XML-u.
- Komunikacja:
 - za pośrednictwem protokołu HTTP, bezpośrednio przez URL,
 - moduł X-Node, zapewniający integrację z innymi źródłami danych:
 - ODBC, OLE DB,
 - system plików.
- Platforma dla:
 - aplikacji internetowych typu B2C,
 - elektronicznej wymiany dokumentów:
 - nowość: wsparcie dla XML Signature;
 - systemów zarządzania treścią:
 - nowości: wersjonowanie, scalanie, indeksowanie dokumentów nie-XML.

Baza danych w Tamino

- Definicja tabeli – XML Schema.
- Wiersz tabeli – element z podelementami.
- Pole – element z zawartością (podelement wiersza).
- Referencja – w XML Schema.
- Zapytanie – w XQuery.

XML w bazach danych – przegląd

Relacyjne ze wsparciem

- Oracle 8i / 9i / 10g
- Microsoft SQL Server 2000
- DB2, IBM
- Sybase ASE 12.5

XML-owe

- Tamino, Software AG
- TEXTML Server, InxiaSoft
- dbXML (open source)
- eXist (open source)
- Xindice, Apache Software Foundation (open source)

Plan

- 1 Bazy danych
 - XML w relacyjnych bazach danych
 - XML-owe bazy danych

- 2 XML w bezpieczeństwie
 - XML Signature
 - XML Encryption

Standardy XML związane z bezpieczeństwem

Za Pawłem Radzińskim

- Podpisy – XML Signature.
- Szyfrowanie – XML Encryption.
- Zastosowanie: m.in. w Web services.

XML Signature

- Podpis dokumentu XML-owego zapisany w postaci struktury XML-owej.
- Podpis umieszczany w elemencie `Signature`:
 - w osobnym dokumencie (*detached signature*),
 - dołączonym do podpisywanego dokumentu (*enveloped signature*),
 - zawierającym podpisywane dane (*enveloping signature*).
- Możliwości XML Signature:
 - podpisywanie fragmentów dokumentu XML,
 - podpisywanie zasobów zewnętrznych (dostępnych poprzez URL),
 - podpisy wielokrotne.

XML Signature – przykład 1 (*detached*)

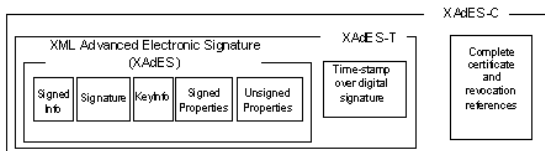
```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm=
      "http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm=
      "http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
    <!-- w URI znajduje się wskazanie na podpisywane dane - tu zewnętrzne -->
    <Reference URI="http://przyklad.pl/pliki/do-podpisu.xml">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#base64"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>60NvZvtdTB+7UnlLp/H24p7h4bs=</DigestValue>
    </Reference>
  </SignedInfo>
  <!-- zaszyfrowany skrót z SignedInfo - podpis -->
  <SignatureValue>OsH9A1jTNL...</SignatureValue>
  <KeyInfo><KeyValue><DSAPublicValue>
    <P>imup6lm...</P><Q>xDve3j7...</Q><G>NlugAf...</G>
    <Y>W7dOmH/v...</Y>
  </DSAPublicValue></KeyValue></KeyInfo>
</Signature>
```

XML Signature – przykład 2 (*enveloped*)

```
<?xml version="1.0" encoding="UTF-8"?>
<Document>
  <Content>
    ...
  </Content>
  <ds:Signature>
    <ds:SignedInfo>
      <ds:Reference URI="">
        <ds:Transforms>
          <ds:Transform
            Algorithm="http://www.w3.org/2000/09/xmldsig
              #enveloped-signature"/>
          </ds:Transforms>
        </ds:Reference>
      </ds:SignedInfo>
      ....
    </ds:Signature>
  </Document>
```

XML Signature - XAdES

- XAdES - XML Advanced Electronic Signature
- Rodzina zaawansowanych formatów podpisu XML
 - informacje pozwalające na przedłużenie ważności podpisu,
 - zgodność z Dyrektywą Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych.



XML Encryption

- Cel: zagwarantowanie poufności danych w XML.
- Szyfrować można zarówno cały plik XML jak i jego części.

```
<purchaseOrder>
<Order>
<Item>book</Item>
  <Id>123-958-74598</Id>
  <Quantity>12</Quantity>
</Order>
<Payment>
  <CardId>123654-8988889-9996874</CardId>
  <CardName>visa</CardName>
  <ValidDate>12-10-2004</ValidDate>
</Payment>
</purchaseOrder>
```

XML Encryption – przykład 1 (fragment)

```
<PurchaseOrder>
  <Order>
    <Item>book</Item>
    <Id>123-958-74598</Id>
    <Quantity>12</Quantity>
  </Order>
  <Payment>
    <CardId>
      <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Content'
        xmlns='http://www.w3.org/2001/04/xmlenc#'>
        <CipherData>
          <CipherValue>A23B45C564587</CipherValue>
        </CipherData>
      </EncryptedData>
    </CardId>
    <CardName>visa</CardName>
    <ValidDate>12-10-2004</ValidDate>
  </Payment>
</PurchaseOrder>
```

XML Signature – przykład 2 (cały dokument)

```
<EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
  Type='http://www.isi.edu/in-notes/iana/
    assignments/media-types/text/xml'>
  <CipherData>
    <CipherValue>A23B45C56</CipherValue>
  </CipherData>
</EncryptedData>
```