Implementasi XML Signature pada Dokumen XML untuk Transkrip Nilai Online

Bernard Renaldy Suteja
Jurusan Teknik Informatika
Fakultas Teknologi Informasi, Univeritas Kristen Maranatha
Jl. Surya Sumantri 65 Bandung
bernard.rs@eng.maranatha.edu, bernardjogja@gmail.com

Abstract

XML as data representation is used for data exchange among various web based applications. XML documents have a structured format and they are machine-useable and human-readable. This causes the XML to have a big chance to be modified, so the data integrity is no longer secure.

In order to keep the integrity, a standard way issued by W3C using XML Digital Signature is needed. There are three types of XML Digital Signature, i.e. Enveloped, Enveloping and Detached. This research applies the two types; Enveloped and Enveloping by using online transcript case and data transcript verification with XML format, witch already has digital signature.

In creating or developing the XML-base next application, it is important to use this security standard to create secure XML.

Keywords *: XML Digital Signature, XML Secure*

1. Pendahuluan

Keberadaan XML untuk representasi data dalam berbagai aplikasi terlebih yang berbasis web (internet) saat ini makin berkembang pesat. Berbeda dengan HTML yang menampilkan data secara tidak terstruktur (karena bertujuan hanya untuk menampilkan informasi saja), XML mampu menampilkan data dalam format terstruktur dan mudah dipahami oleh aplikasi ataupun manusia (*application-human usable*). XML dibangun untuk memudahkan dalam proses pengolahan ataupun kombinasi (pertukaran) terhadap data.

Dikarenakan sifat keterbukaan dari dokumen XML itu sendiri (mudah diakses – dibaca dan diubah) dan media internet yang memungkinkan setiap komputer yang terhubung dapat dengan mudah saling bertukar data – informasi, menyebabkan munculnya berbagai masalah khususnya mengenai keamanan (*security*). Aspek keamanan memiliki peran yang sangat penting di dunia internet untuk memberikan kepastian mengenai keaslian materi (*content*) dan transaksi dalam bisnis, memberi perlindungan kerahasiaan dan menjamin informasi digunakan secara benar. Saat data dokumen XML dikirim dalam jaringan (internet), peranan kriptografi adalah untuk merahasiakan data dengan menggunakan enkripsi dan untuk kemudian akan didekripsi oleh penerima. Akan tetapi kriptografi tidak dapat menjamin bahwa data tersebut memang dibuat oleh pengirim yang sesungguhnya (tidak ada bukti otentik sehingga akan terjadi penyangkalan) dan juga tidak dapat menjamin kepastian mengenai keaslian materi (integritas). Salah satu cara untuk menjaga keaslian data pada dokumen XML yang diangkat dalam penelitian ini adalah dengan menggunakan XML Digital Signature dengan kasus Transkrip Online, sehingga integritas informasi transkrip tetap terjaga.

2. Landasan Teori

2.1 Rekomendasi untuk XML *Secure*

Keamanan selalu menjadi hal yang amat penting khususnya dalam dunia internet. Karena data yang ditransaksikan harus terjaga [Fre02] :

1. Integritas
   Data (dokumen XML) tidak diubah sejak dari pengiriman hingga sampai ke penerimanya.
2. Autentikasi
   Keasliaan data yang menyatakan asal dari pengirim yang sesungguhnya.
3. Kerahasiaan
   Kerahasiaan data yang dikirimkan oleh si pengirim, melibatkan algoritma kriptografi.

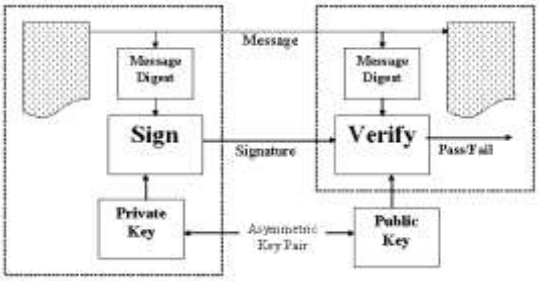
Dengan berpegang pada aturan keamanan data tersebut, maka untuk sebuah XML dokumen yang memiliki sifat terbuka (berbasis pada teks) sehingga dapat dibaca dan diubah dapat menggunakan standart keamanan XML sebagai berikut :

1. *XML Digital Signature* untuk integritas dan keaslian
2. *XML Encryption (XML Enc)* untuk kerahasiaan
3. *XML Key Management (XKMS)* untuk pengaturan kunci
4. *Security Assertion Markup Language* (*SAML*) berkenaan dengan autentifikasi
5. *XML Access Control Markup Language* (*XACML*) berkenaan dengan aturan mengenai otorisasi

W3C merekomendasikan penggunaan kelima standart tersebut, sedangkan standart yang paling sering digunakan adalah *XML Digital Signature* dan *XML Encryption*.

2.2 XML Digital Signature

Digunakan untuk menyediakan kepastian terhadap integritas data (*content of message*) dalam dokumen serta membuat *digest* data dan menguji tanda tangan elektronik tersebut (*digital signature*). Dengan cara ini kepastian terhadap integritas data dapat terjamin, *user* dapat mendeteksi perubahan isi yang tidak diharapkan, baik karena faktor kesengajaan atau yang lainnya. Tanda tangan digital ini menghubungkan data dengan penandaan data (*message digest*) serta digunakannya teknik kriptografi berupa enkripsi dan dekripsi [Eas03].



Gambar 1. *Digital Signature Flowchart*

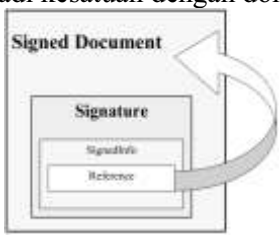
Tanda tangan digital memiliki kesamaan sifat dengan tanda tangan konvensional sehingga dapat dipakai untuk berbagai tujuan. Struktur dari XML digital signature [Rea99] adalah :

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod />
```

```
    <SignatureMethod>
    <Reference URI>
      <DigestMethod> </DigestMethod>
      <DigestValue> </DigestValue>
    </Reference>
  </SignedInfo>
 <SignatureValue> </SignatureValue>
 <KeyInfo> </KeyInfo>
 </Signature>
```

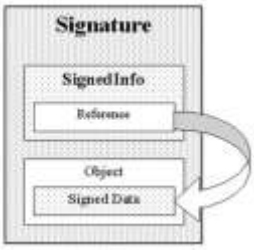
Berdasarkan pada letak *digital signature*-nya maka dalam *XML digital signature* terdapat tiga tipe [Eas03], yaitu :

1. *Enveloped Signature*
   Tanda tangan diletakkan menjadi kesatuan dengan dokumen XMLnya.



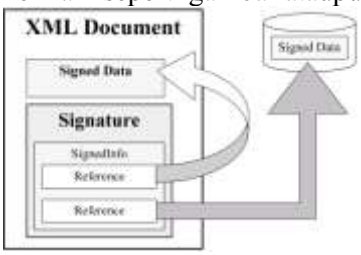
Gambar 2. Skema *Enveloped Digital Signature*

2. *Enveloping Signature*
   Tanda tangan menjadi elemen utama dokumen XML dan datanya sendiri merupakan bagian dari elemen tanda tangan tersebut.



Gambar 3. Skema *Enveloping Digital Signature*

3. *Detached Signature*
   Digunakan untuk menandatangani dokumen XML yang berasal pada lokasi terpisah atau sebuah dokumen lain seperti gambar ataupun HTML.



Gambar 4. Skema *Detached Digital Signature*

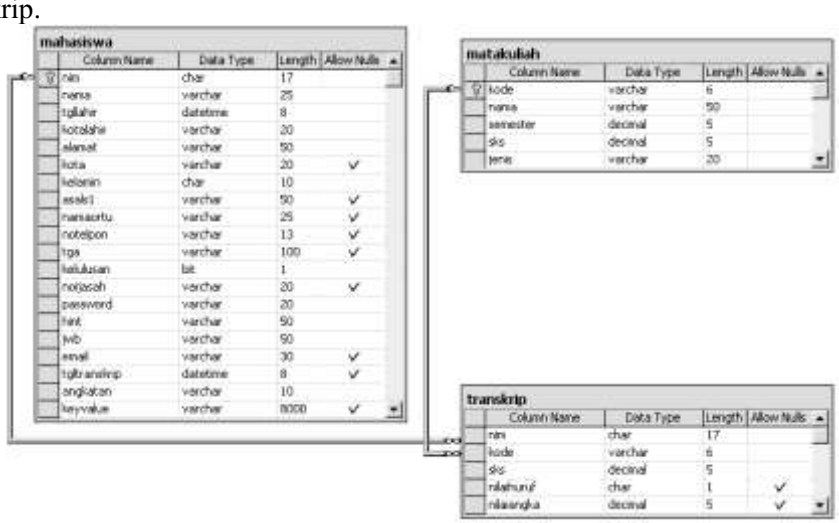
3. Metode Penelitian

Penelitian yang diangkat, dikhususkan pada sisi integritas data dokumen XML yang merupakan transkrip online. Adapun cara yang ditempuh adalah melalui pengimplementasian XML Digital Signature. Berikut adalah tahap-tahap untuk menyajikan informasi berupa dokumen XML yang telah disignature, sehingga integritasnya dapat terjaga.

3.1 Query data ke database untuk Transkrip Online dengan format XML

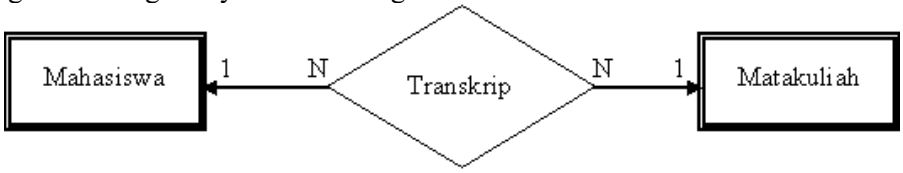
XML (*Extensible Markup Language*) merupakan bahasa yang mendefinisikan struktur data dan value dari suatu informasi yang dikemas dalam bentuk sebuah dokumen. XML juga dapat digunakan untuk menjelaskan secara virtual berbagai jenis informasi, untuk itulah maka dikatakan *extensible*. Dokumen XML terbagi menjadi dua kategori, yaitu well-form dan valid XML. Well form adalah XML yang tidak melibatkan pendefinisian struktur tipenya (sederhana). Untuk sebuah dokumen XML yang valid maka haruslah telah menjadi dokumen XML yang well form. Sedangkan untuk valid XML itu sendiri harus mengikutsertakan definisi tiap tipenya (DTD = *Document Type Definition*) yang mendefinisikan struktur dokumen, dan dokumen harus menaati struktur yang didefinisikan dalam DTD tersebut. Penggunaan DTD dapat secara internal dalam dokumen XML yang bersangkutan atau eksternal terpisah dari dokumen XML.
Database yang merupakan kumpulan dari beberapa data (*record*) terorganisir dalam tabel-tabel (*entity*).

Contoh kasus:
Sebuah database terdiri dari tiga entitas utama yaitu mahasiswa, matakuliah, dan transkrip.



Gambar 5. Kamus Data

Dengan ER Diagramnya adalah sebagai berikut :



Gambar 6. ER Diagram

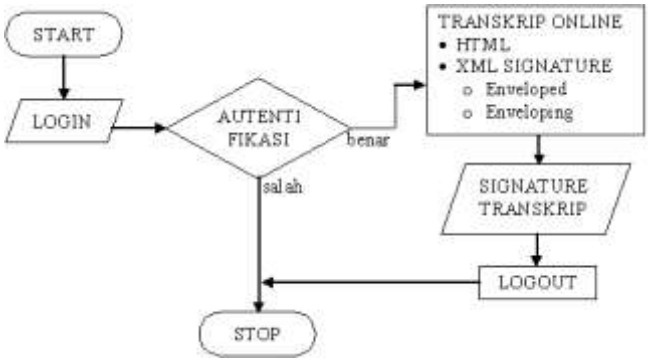
Hasil informasi transkrip online dengan format XML akan memiliki susunan elemen tag berikut :

```
<DATA_MHS>
<NIM_MHS></NIM_MHS>
<NAMA_MHS></NAMA_MHS>
<TGL_TRANSKRIP></TGL_TRANSKRIP>
<JUDUL_SKRIPSI></JUDUL_ SKRIPSI >
<NO_IJAZAH></NO_IJAZAH>
<DATA_MATA_KULIAH>
<KD_MATAKULIAH></KD_MATAKULIAH>
<NM_MATAKULIAH></NM_MATAKULIAH>
<DATA_NILAI>
<BOBOT_SKS></BOBOT_SKS>
<NILAI></NILAI>
</DATA_NILAI>
</DATA_MATA_KULIAH>
 ...
<INDEK_PRESTASI>
<TOTAL_SKS></TOTAL_SKS>
<ANGKA_KUALITAS> </ANGKA_KUALITAS>
<IPK></IPK>
</INDEK_PRESTASI>
</DATA_MHS>
```

3.2 Algoritma dan Flowchart Sistem

Sistem yang dirancang, digunakan untuk menghasilkan XML yang *secure* dengan menerapkan *XML Digital Signature* yang bertipe *Enveloped Signature* dan *Enveloping Signature*, serta sistem dapat juga digunakan untuk melakukan verifikasi terhadap integritas dokumen XML yang telah di-*signature*. Sistem yang dibuat menggunakan *namespace* dari .Net *Framework* yaitu ***System.Security.Cryptography.Xml*** dengan kelas ***SignedXML***.

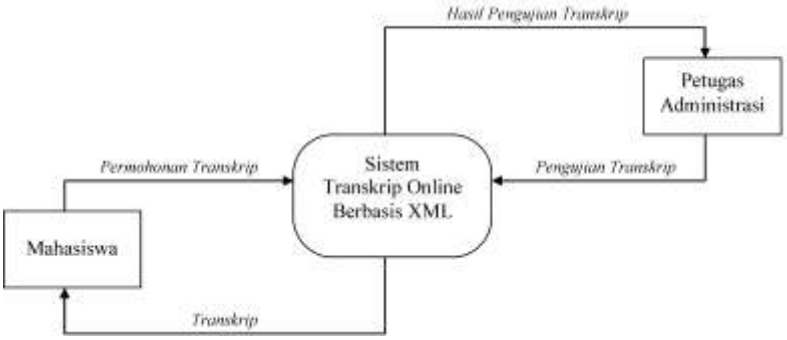
Mahasiswa yang akan mengakses transkrip online harus melakukan autentifikasi terlebih dahulu dengan mengisikan NIM (Nomor Induk Mahasiswa) disertai dengan Passwordnya, untuk selanjutnya mahasiswa dapat mengakses transkripnya dan dapat memperolehnya dalam bentuk *XML Secure* yang mengimplementasikan *Digital Signature*.



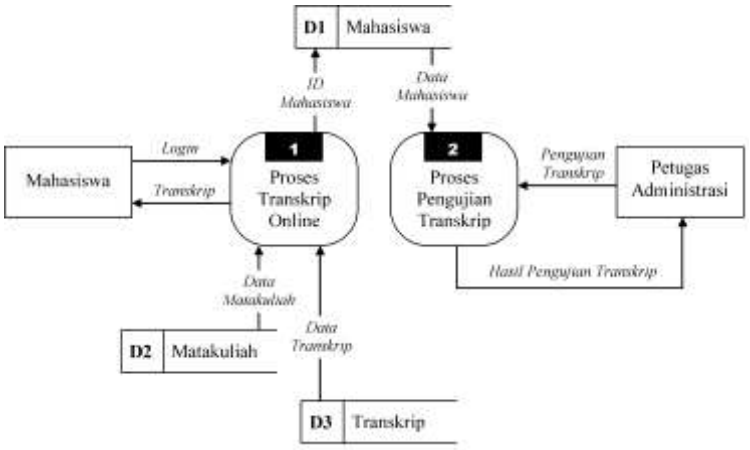
Gambar 7. Flowchart Sistem

3.2.1 Data Flow Diagram

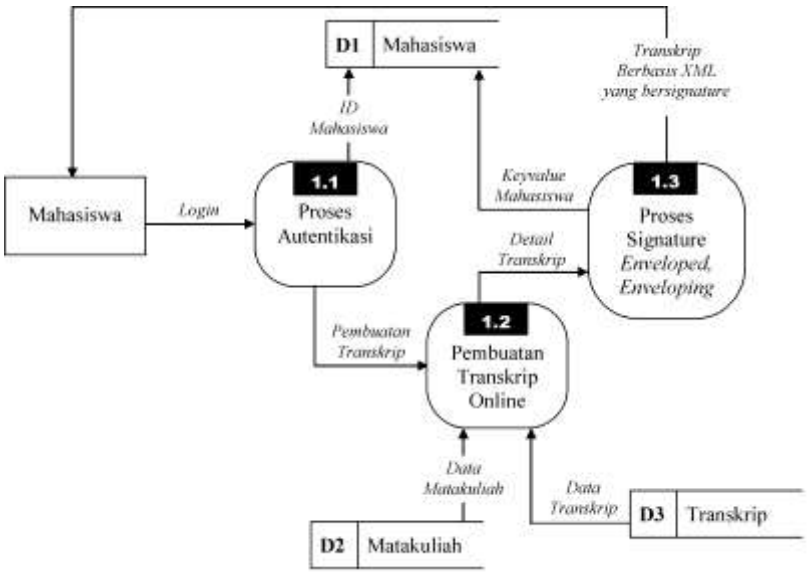
Data Flow Diagram (DFD) sistem ini terbagi menjadi dua *level*. Masing – masing level dari diagram ini akan menunjukan keseluruhan maupun secara lebih terinci mengenai transkrip online. *Level* nol merupakan pelevelan secara keseluruhan dari sistem. *Level* 1 merupakan penurunan dari *Level* 0 yang berisi semua event – event dari seluruh sistem informasi transkrip online, dan *Level* 2 merupakan penurunan *Level* 1 yang berisi tentang proses terbentuknya transkrip online. Adapun DFD masing-masing *level* adalah sebagai berikut :



Gambar 8. Data Flow Diagram Level 0



Gambar 9. *Data Flow Diagram Level 1*

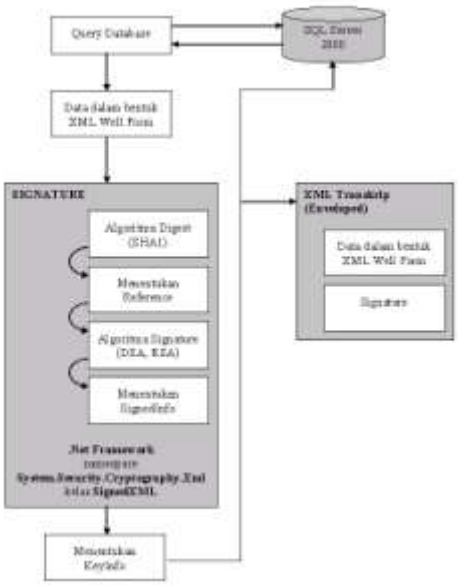


Gambar 10. *Data Flow Diagram Level 2*

3.2.2 *Enveloped Signature*

Proses *signature* dokumen XML dengan menggunakan type enveloped diawali dari menerima informasi untuk transkrip yang diquery ke database, sesuai dengan data mahasiswa yang bersangkutan. Selanjutnya data tersebut diubah kedalam format XML dokumen yang well form. Hasil tersebut akan menjadi element anak yang akan menjadi *reference* dari *XML Digital Signature*.

Reference tersebut untuk selanjutnya akan di *digest* dan diperoleh *digest value*. Baik *reference* dan *digest* tersebut akan berada sebagai kesatuan element yang disebut *SignedInfo* untuk kemudian dengan dilakukan proses *canonicalization* dan *Signature* sesuai dengan algoritma yang dipilih terhadap element *SignedInfo* tersebut, hasilnya akan ditempatkan pada element S*ignatureValue* dengan menyertakan pula attribut dari kunci (*keyvalue*), yang kemudian disimpan dalam database.

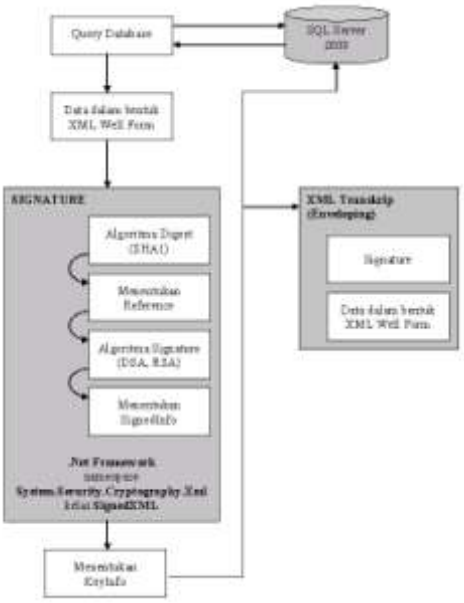


Gambar 11. *Flowchart Signature Type Enveloped*

Hasil *Signature* yang berada pada *element Signature* tersebut akan disatukan ke dokumen XML awal sebagai element anak yang terakhir.

3.2.3 *Enveloping Signature*

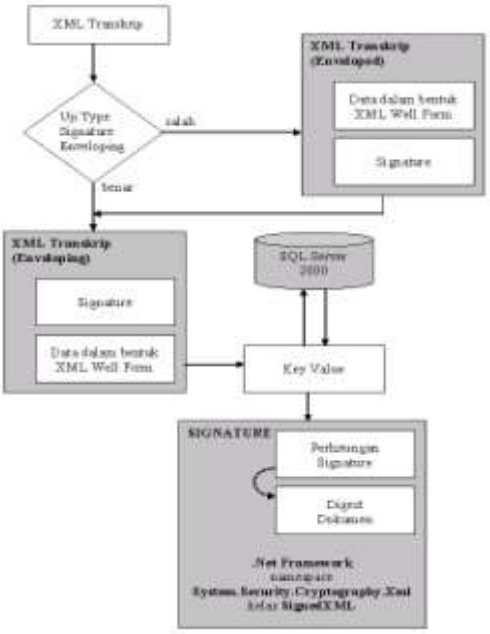
Proses *signature* dokumen XML dengan menggunakan type *enveloping* hampir sama dengan proses *enveloped*, yaitu diawali dari menerima informasi untuk transkrip yang di-*query* ke database, sesuai dengan data mahasiswa yang bersangkutan. Selanjutnya data tersebut diubah kedalam format xml dokumen yang *well form*. Hasil tersebut akan menjadi element anak yang akan menjadi *reference* dari *XML Digital Signature*. *Reference* tersebut untuk selanjutnya akan di *digest* dan diperoleh *digest value*. Baik *reference* dan *digest* tersebut akan berada sebagai kesatuan *element* yang disebut *SignedInfo* untuk kemudian dengan dilakukan proses *canonicalization* dan *Signature* sesuai dengan algoritma yang dipilih terhadap element *SignedInfo* tersebut hasilnya akan ditempatkan pada *element SignatureValue* dengan menyertakan pula attribut dari kunci (*keyvalue*), yang kemudian disimpan dalam database. Hasil *Signature* yang berada pada *element Signature* (menjadi elemen *root*) tersebut akan memperoleh element anak berupa *Object* yang merupakan Signature property yang berisi dokumen XML awal sebagai element anak



Gambar 12. Flowchart *Signature Type Enveloping*

3.2.4 Verifikasi *Signature*

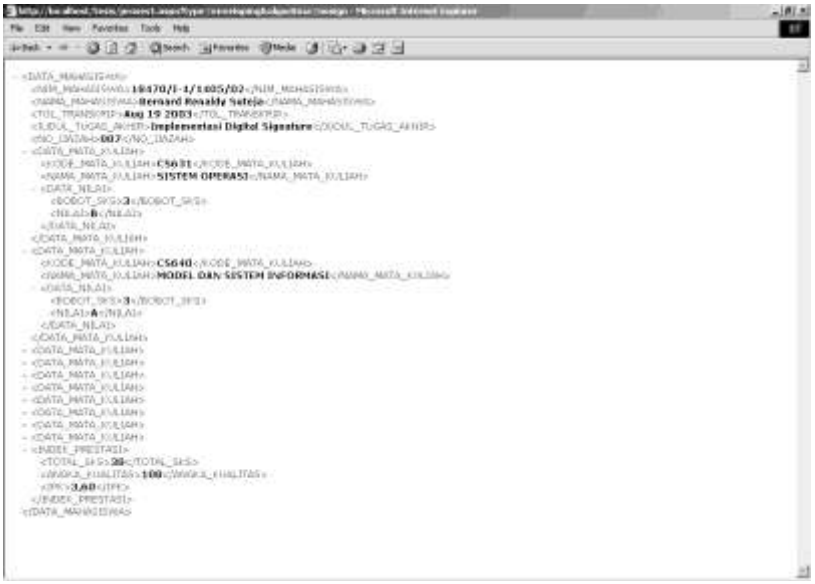
Pada proses verifikasi *signature* ini dapat dideteksi secara otomatis tipe *signature* yang ada pada dokumen XML (transkrip). Untuk melakukan verifikasi terhadap dokumen XML secure yang menerapkan digital signature, diawali dari menerima dokumen xml yang telah disignature tersebut kemudian mengambil informasi dari *element Signature*. Sehingga akan diperoleh terpisah antara Signature dengan data (*Object*). Kemudian dilakukan proses pengujian signature beserta datanya sesuai dengan algorima digest dan signature yang dipilih. Elemen <*SignatureValue*> harus sesuai dengan hasil perhitungan terhadap elemen <*SignedInfo*> dengan menggunakan algoritmanya serta informasi kunci (*keyvalue*) yang ada dalam database. Selanjutnya dilakukan proses pengecekan digest terhadap data yang kemudian dibandingkan dengan elemen <*DigestValue*> menggunakan algoritma digestnya. Jika integritas data yang dihasilkan dari proses tersebut masih terjaga maka dapat dipastikan belum terjadi modifikasi terhadap dokumen XML tersebut. Sebaliknya jika tidak adanya integritas data yang dihasilkan dari proses tersebut maka modifikasi terhadap dokumen XML tersebut telah terjadi.



Gambar 13. Flowchart *Verifikasi Signature*

4. Hasil dan Pembahasan

Proses yang paling inti dalam sistem ini adalah proses memperoleh transkrip nilai. Untuk memperoleh transkrip yang memiliki type format XML yang terdapat digital signaturenya maka pada tampilan halaman transkrip dapat dipilih algoritma *NoSignature*, *DSAwithSHA1* atau *RSAwithSHA1* untuk message digest yang akan diberikan pada elemen *Reference* nantinya serta algoritma *signature*-nya, pilihan tersebut berdasarkan pada standar rekomendasi dari W3C. Selanjutnya penentuan type penyajian *signature*-nya (tipe dari *XML Digital Signaturenya*), pilihannya adalah *Enveloped* atau *Enveloping*. Hasil dari transkrip yang bertipekan *XML Digital Signature* ini dapat disimpan untuk kemudian dapat digunakan sebagai transkrip nilai digital.



Gambar 15. Transkrip XML tanpa mengimplementasikan XML Digital Signature

Gambar 16. Transkrip *XML Digital Signature* dengan *DSAwithSHA1 type Enveloped*

Gambar 17. Transkrip *XML Digital Signature* dengan *DSAwithSHA1 Type Enveloping*

Gambar 18. Transkrip *XML Digital Signature* dengan *RSAwithSHA1 Type Enveloped*

Gambar 19. Transkrip *XML Digital Signature* dengan *RSAwithSHA1 Type Enveloping*

Jika terjadi modifikasi dokumen Transkrip XML tersebut baik data maupun Signaturenya maka integritas dokumen XML tidak terjaga, hal ini dapat diketahui karena proses verifikasi akan memberikan kembalian nilai *false*.

5. Kesimpulan

Hasil dari mengimplementasikan XML Signature untuk memperoleh dokumen XML yang *secure* pada kasus transkrip online ini, sesuai dengan tujuan penulisan sehingga diperoleh kesimpulan sebagai berikut :

1. Dokumen XML memiliki sifat *application-human-usable* sehingga tidak sensitif terhadap modifikasi data dengan demikian integritas data tidak dapat dijaga dengan menggunakan *XML Digital Signature* yang sangat sensitif terhadap adanya modifikasi data maka integritasnya tetap bisa dipertahankan.
2. Pengimplementasiaan *XML Digital Signature* dengan *type Enveloped* atau *Enveloping* lebih mudah dilakukan dan lebih baik karena hasilnya menjadi satu dengan data-data dokumen XMLnya yang diperoleh dengan melakukan query data pada database.
3. Dengan mengimplementasikan *XML Digital Signature* ini, maka informasi yang bersifat konvensional seperti transkrip dapat digantikan dengan menggunakan transkrip online yang berbasis XML dengan mengimplementasikan *XML Digital Signature*.
4. Penggunaan standar pada dokumen XML yang mengimplementasikan *XML Digital Signature* akan menjadi pedoman baku dan memudahkan, dalam membuat ataupun mengembangkan aplikasi yang menggunakan dokumen XML tersebut selanjutnya.

6. Saran

Untuk mengimplementasikan *XML Signature* sehingga diperoleh dokumen XML yang *secure* pada kasus transkrip online ini, ada beberapa saran-saran yang dapat digunakan pada pengembangan selanjutnya yaitu sebagai berikut :

1. Dokumen XML yang akan disignature tidak hanya kategori well-form saja tetapi juga valid yang melibatkan Data Type Definitions (DTD).
2. Lebih banyak pilihan algoritma untuk Signature dan Message Digestnya, tidak hanya yang direkomendasikan oleh W3C saja tetapi dapat pula dari algoritma yang lain.
3. Pengembangan XML Digital Signature dengan type Detached untuk source data yang type formatnya bervariasi dan perlu dipertimbangkan adanya resource yang memadai.
4. Pengimplementasian standar keamanan lain yang telah direkomendasikan sangat perlu untuk diterapkan semua agar memperoleh secure XML. Proses penerapan standar tersebut ada baiknya secara bertahap.

Daftar Pustaka

[Eas03] *Eastlake D. E. XML Security. Available: http://www.motorola.com. Accessed: 22 January 2003. 10:20:52.*

[Ed03] *Ed S. Paul Madsen. Carlisle Adams. An Introduction to XML Digital Signatures. Available: http://www.xml.com/pub/a/2001/08/08/xmldsig.html. XML.com. Accessed:15 Mei 2003. 11:07:22.*

[Fre02] *Frederick H. Available: http://www.sitepoint.com/article/933/. Accessed: 28 November 2002. 11:20:33.*

[Mac03] *Mactaggart M. Enabling XML security. Available:http://www-106.ibm.com/developerworks/xml/library/s-xmlsec.html/index.html. IBM. Accessed:21 Mei 2003. 19:14:38.*

[Man03] *Manoj K. S. SecureXML(tm) Digital Signature Verification Web Service Launched. Available:http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd. W3C. Accessed:21 Mei 2003. 19:13:56.*

[Mar03] *Mark B., John Boyer, Barb Fox, Brian LaMacchia, Ed Simon. XML-Signature Syntax and Processing. Available:http://www.w3.org/TR/xmldsig-core/. W3C. Accessed:21 Mei 2003. 18:50:32.*

[Rea99] *Reagle J. XML-Signature Requirements. 1999. Available:http://www.w3.org/TR/xmldsig-requirements. W3C. Accessed:21 Mei 2003. 19:12:46.*