Implementasi Tanda Tangan Digital pada Partitur Musik MusicXML

Hafid Inggiantowi / 13507094
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if17094@students.if.itb.ac.id

***Abstrak*—Tanda tangan digital (*digital signature*) telah diakui sebagai suatu metode yang dapat memastikan kebenaran daripada suatu dokumen. Partitur musik merupakan karya, hasil kerja keras, dan kreativitas daripada seseorang yang merupakan suatu penggubah musik. Partitur musik kini sering dituliskan dalam format penulisan musik yang secara luas digunakan di dunia yaitu MusicXML. MusicXML ini memungkinkan distribusi partitur musik yang lebih mudah dengan jaringan internet. Dengan semakin berkembangnya penggunaan pada internet, tanda tangan digital dapat diterapkan sebagai metode pengamanan pada partitur MusicXML sehingga hanya pihak tertentu yang diinginkan yang dapat menggunakannya.**

***Kata Kunci*— tanda tangan digital, partitur musik, *MusicXML*.**

I. LATAR BELAKANG

Tanda tangan digital (*digital signatures*) merupakan suatu cara yang digunakan untuk mengidentifikasi dan melakukan validasi atas suatu dokumen yang berisikan informasi. Tanda tangan digital memberikan penggunanya alasan untuk percaya bahwa pesan yang ia terima merupakan pesan yang asli dan berasal dari pengirim yang ia ketahui. Tanda tangan digital digunakan secara umum untuk perangkat lunak terdistribusi, transaksi keuangan, dan kasus lain yang penting untuk mendeteksi keaslian. Sekarang ini, tanda tangan digital telah banyak digunakan untuk aspek keamanan seperti penanganan masalah kerahasiaan pesan, otentikasi, keaslian pesan, dan nirpenyangkalan.

Partitur musik kini sering dituliskan dalam format standar musik dunia yang sering digunakan yang bernama MusicXML. Tanda tangan digital untuk partitur MusicXML dapat dilakukan dengan berbagai metode yang telah diakui merupakan salah satu algoritma validasi dan verifikasi sebuah dokumen MusicXML tersebut. Tanda tangan digital akan dimiliki unik oleh setiap dokumen MusicXML.

Kita ketahui bahwa MusicXML ini juga dikembangkan atas dasar kemudahan distribusi filenya pada internet. Dengan semakin berkembangnya penggunaan internet, membuat pendistribusian partitur musik semakin mudah sehingga setiap orang dapat menggunakan partitur musik tersebut tanpa seizin pembuatnya. Hal ini membuat sebagian besar penggubah partitur perlu untuk membatasi hak penggunaannya sehingga hanya pihak tertentu yang berhak yang dapat menggunakannya. Adanya tanda tangan digital juga dapat mencegah terjadinya distribusi yang tidak tepat sasaran. Tanda tangan digital juga dapat digunakan untuk memastikan bahwa partitur yang dikirimkan tidak berubah dari yang dikirimkan.

Adapun salah satu metode tanda tangan digital yang dapat diimplementasikan adalah tanda tangan digital dengan menggunakan XML. Tanda tangan digital XML merupakan salah satu cara khusus yang dapat diterapkan pada setiap data berstruktur XML. Tanda tangan tersebut dapat diterapkan pada sebagian daripada dokumen XML. Tanda tangan digital XML memiliki beberapa standar yang dispesifikasikan dalam *XML-Signature Syntax and Processing Specification* (XML DSIG).

Makalah ini akan membahas mengenai bagaimana suatu partitur MusicXML yang merupakan suatu dokumen XML dapat dilakukan implementasi tanda tangan digital, yang kemudian akan dapat diperiksa verifikasinya. Makalah ini juga membahas bagaimana tanda tangan digital pada partitur MusicXML dapat menjadi metode pengamanan untuk pengembangan format tersebut. Pada tulisan ini, penulis mencoba memberikan usulan implementasi ide tanda tangan digital pada partitur MusicXML. Implementasi dilakukan dengan salah satu algoritma tanda tangan digital yaitu RSA. Dengan demikian, tanda tangan digital pada MusicXML dapat digunakan untuk mencegah terjadinya klaim kepemilikan partitur oleh seseorang. Terdapat dua usulan, yaitu pembuatan tanda tangan digital langsung non XML serta pembuatan tanda tangan dalam bentuk tanda tangan digital XML.

II. TANDA TANGAN DIGITAL (*DIGITAL SIGNATURE*)

Tanda tangan digital (*digital signature*) merupakan skema matematis untuk membuktikan keautentikan dari suatu pesan atau dokumen digital. Tanda tangan digital yang dimaksud disini bukanlah tanda tangan seseorang yang di-dijitasi dengan alat *scanner* sebagai tanda tangan pada dokumen digital. Tanda tangan digital ini merupakan

suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan. Teknik yang umum digunakan dalam membentuk tanda tangan digital adalah dengan memanfaatkan fungsi *hash* serta melibatkan algoritma kriptografi kunci publik.

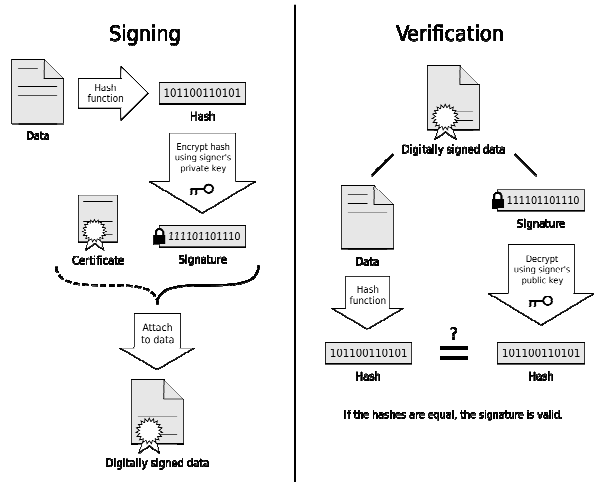
Teknologi tanda tangan digital yang memanfaatkan teknologi kunci publik dapat dijelaskan sebagai berikut. Sepasang kunci publik-privat dibuat untuk keperluan seseorang. Kunci privat disimpan oleh pemiliknya, dan dipergunakan untuk membuat tanda tangan digital, sedangkan kunci publik dapat diserahkan kepada siapa saja yang ingin memeriksa tanda tangan digital yang bersangkutan pada suatu dokumen.

Tanda tangan digital dapat digunakan untuk jenis pesan apapun, baik itu terenkripsi atau tidak, sehingga penerima dapat memastikan identitas dari pengirim dan pesan yang diterima tiba dengan utuh. Sertifikat digital yang berisi tanda tangan digital mengandung otoritas sertifikasi sehingga siapapun dapat melakukan verifikasi untuk memeriksa bahwa sertifikasi itu adalah asli. Sehingga demikian, tanda tangan digital dapat digunakan untuk menjamin integritas daripada suatu dokumen atau pesan.

Beberapa sifat yang dimiliki oleh tanda tangan digital adalah:

- Otentik, tidak bisa/sulit ditulis/ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penandatangan tak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya.
- Hanya sah untuk dokumen (pesan) itu saja atau salinannya yang sama persis. Tanda tangan tersebut tidak bisa dipindahkan ke dokumen lainnya, meskipun dokumen lain itu hanya berbeda sedikit. Ini juga berarti bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak lagi sah.
- Dapat diperiksa dengan mudah, termasuk oleh pihak-pihak yang belum pernah bertatap muka langsung dengan penandatangan.

Skema umum tanda tangan digital dapat dilihat pada Gambar 1.



Gambar 1 Skema penandatanganan digital

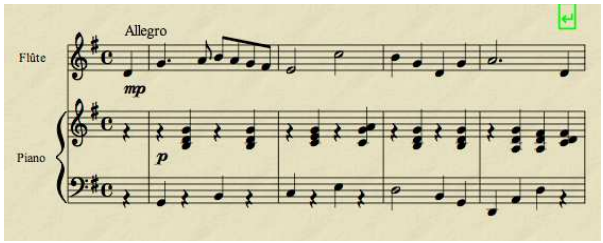
Skema penandatanganan digital terdiri dari 3 proses, antara lain yaitu :

1. Proses pembangkitan kunci. Proses ini memilih kunci privat secara acak dari kumpulan kunci privat yang mungkin. Hasil daripada proses ini adalah kunci privat dan kunci publik yang saling sesuai.
2. Proses pemberian tanda tangan. Proses ini menerima isi pesan dan kunci privat, sehingga menghasilkan tanda tangan. Hal ini dilakukan dengan mengenkripsi nilai *hash* daripada isi pesan tersebut.
3. Proses verifikasi tanda tangan. Proses ini memverifikasi pesan yang telah terbubuhi tanda tangan digital. Proses verifikasi ini membutuhkan kunci publik.

Terdapat beberapa algoritma tanda tangan digital yang dapat digunakan, antara lain seperti RSA, DSA dan varian *elliptic curve*-nya yaitu ECDSA, ElGamal, Rabin, dan lain sebagainya. Algoritma yang dapat digunakan untuk pembuatan tanda tangan adalah RSA dan SHA-1, yang dispesifikasikan lebih lengkap pada pustaka [8] dan [9]. Pada bagian analisis, algoritma inilah yang akan digunakan.

III. MUSICXML

MusicXML merupakan format musik yang dikembangkan oleh Recordare, LLC. MusicXML ini bersifat *internet-friendly* sehingga memungkinkan pecinta musik mudah mendapatkan musik secara *online*. Saat ini banyak perangkat lunak musik yang sudah mendukung MusicXML sebagai salah satu format yang dapat diolah. Beberapa mendukungnya secara *native*, yang lain mendukungnya melalui *plug-in* atau *extension* yang disediakan pengembangnya atau pihak ketiga. Spesifikasi MusicXML dipublikasikan oleh Recordare di http://www.recordare.com/musicxml/specification dalam format MusicXML DTD (*Document Type Definition*), MusicXML XSD, serta XSLT *stylesheets*. Recordare mengeluarkan spesifikasi tersebut di bawah lisensi pemakaian MusicXML *Document Type Definition Public License Version* 2.0 yang mengizinkan penggunaan MusicXML secara bebas. MusicXML umumnya merepresentasikan penulisan partitur dengan menggunakan notasi not balok yang merupakan notasi musik universal yang digunakan di seluruh dunia. Contoh penulisan partitur dapat dilihat pada Gambar 2.



Gambar 2 Partitur pada suatu perangkat lunak penulis musik

Struktur MusicXML dapat dilihat pada Gambar 3. MusicXML biasa dituliskan dalam bentuk *partwise*. Tiap baris instrument didefinisikan oleh tag *part*. *Part* diurutkan secara serial, dan terdiri dari bar-bar yang didefinisikan oleh tag *measures*. *Measures* mengandung elemen-elemen tag sebagai berikut :

1. *Note*
   Note merepresentasikan nada/not atau tanda istirahat. *Note* merupakan *item* yang memiliki nilai durasi tertentu.
2. *Attribute*
   Attribute mendefinisikan *item* yang tidak memiliki durasi seperti tangga nada, kunci, birama, dan sebagainya.
3. *Direction*
   Direction mendefinisikan dinamika.
4. *Sound*
   Sound mendefinisikan tempo.

```
<score-partwise>
      <identification>...</identification>
      <part-list>...</part-list>
      <part id="p1">
          <measure number="1">
              <attributes>...</attributes>
              <note>...</note>
              <note>...</note>
              <note>...</note>
              <note>...</note>
          </measure>
          <measure number="2">
              <note>...</note>
              <note>...</note>
          </measure>
      </part>
      <part id="P2">...</part>
</score-partwise>
```

Gambar 3 Struktur MusicXML

IV TANDA TANGAN DIGITAL XML

Tanda tangan digital XML dispesifikasikan pada *XML-Signature Syntax and Processing Specification* (XML DSIG). Tanda tangan digital XML dapat menandatangani data jenis apapun, biasanya yaitu dokumen XML, tetapi segala sesuatu yang dapat diakses melalui URL juga dapat ditandatangani.

Tanda tangan digital XML yang digunakan untuk menandatangani *resource* di luar dari dokumen XML yang mengandung *resource* tersebut disebut dengan tanda tangan terpisah (*detached signature*). Sedangkan, jika digunakan untuk menandatangani beberapa bagian dari dokumen yang mengandung *resource* tersebut, disebut dengan tanda tangan yang menyelimuti (*enveloping signature*), sedangkan jika dokumen berisi data yang telah ditandatangan di dalamnya maka disebut dengan tanda tangan yang diselipkan (*enveloped signature*).

Struktur tanda tangan digital XML yang dispesifikasikan tersebut dapat dilihat pada Gambar 4.

```
<Signature>
<SignedInfo>
   <CanonicalizationMethod />
      <SignatureMethod />
      <Reference>
         <Transforms>
         <DigestMethod>
         <DigestValue>
      </Reference>
      <Reference /> etc.
 </SignedInfo>
 <SignatureValue />
 <KeyInfo />
 <Object />
</Signature>
```

Gambar 4 Struktur Tanda Tangan Digital XML

Elemen *SignedInfo* berisi data yang ditandatangani dan spesifikasi algoritma apa yang digunakan. Elemen *SignatureMethod* dan *Canonicalization Method* digunakan oleh elemen *SignatureValue* dan tercakup dalam *SignedInfo* untuk perlindungan terhadap gangguan. Satu atau lebih elemen *Reference* berisi spesifikasi *resource* yang ditandatangani oleh *URI Reference,* dan transformasi apapun yang dapat diaplikasikan pada *resource* sebelum ditandatangani. *DigestMethod* berisi spesifikasi algoritm *hash* sebelum mengaplikasikan *hash* tersebut. *DigestValue* berisi hasil daripada algoritma *hash* ke *resource* yang ditransformasi. Elemen *SignatureValue* berisi hasil tanda tangan dalam Base64, tanda tangan ini dibangkitkan dengan parameter yang spesifikasinya berada pada elemen *SignatureMethod.*

Elemen *KeyInfo* merupakan elemen yang secara opsional memungkinkan penandatangan menyediakan penerima dengan kunci yang dapat memvalidasi tanda tangan tersebut, biasanya dalam bentuk sertifikat digital X.509. Elemen *Object* merupakan elemen opsional yang berisi data yang ditandatangan jika tanda tangan yang digunakan merupakan tanda tangan yang diselipkan.

Tanda tangan digital XML ini akan dianalisis sebagai metode untuk mengimplementasikan tanda tangan digital pada partitur MusicXML.

V. ANALISIS IMPLEMENTASI TANDA TANGAN DIGITAL PADA PARTITUR MUSICXML

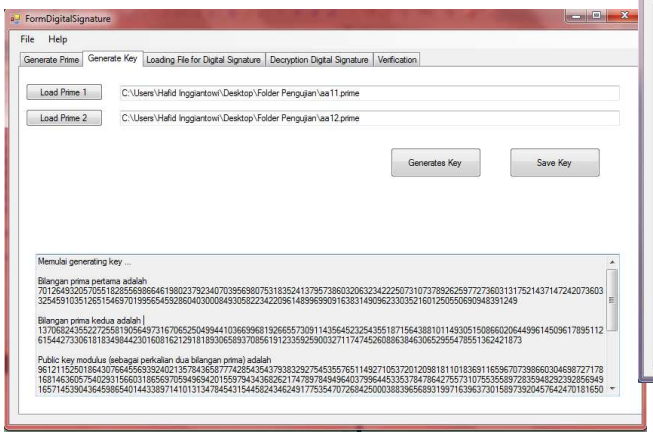
Dalam menyelesaikan masalah verifikasi partitur musik dengan format MusicXML, maka dapat diusulkan untuk mengembangkan suatu aplikasi yang dapat menyisipkan tanda tangan digital dalam partitur MusicXML tersebut ataupun membuat tanda tangan digital dalam file terpisah.

Secara umum, terdapat dua metode usulan yang dapat digunakan untuk membubuhkan tanda tangan digital pada partitur MusicXML ini. Yang pertama, adalah membuat aplikasi berbasis *desktop* sederhana yang dapat membuat

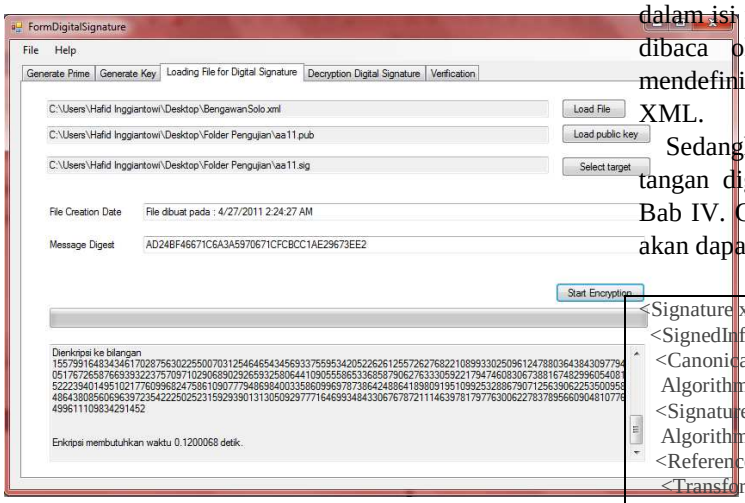
tanda tangan digital untuk jenis file apapun, kemudian menyimpan tanda tangan digital tersebut pada file terpisah. Isi file dapat merupakan heksadesimal atau merupakan *stream* hasil enkripsi dari file.

Sebagaimana pada Gambar 1, program yang dikembangkan ini berjalan mengacu pada skema tersebut. Algoritma yang digunakan untuk program ini adalah SHA-1 dan RSA. Antarmuka yang digunakan untuk pembangkitan kunci dapat dilihat pada Gambar 4. Pada antarmuka ini, pembangkitan kunci dilakukan dengan memasukkan kedua bilangan prima.

Antarmuka yang digunakan untuk membuat tanda tangan dapat dilihat pada Gambar 5. Pada antarmuka ini, akan dibutuhkan kunci publik beserta file partitur MusicXML yang akan dibuat tanda tangan digitalnya.



Gambar 5 Antarmuka pembangkitan kunci

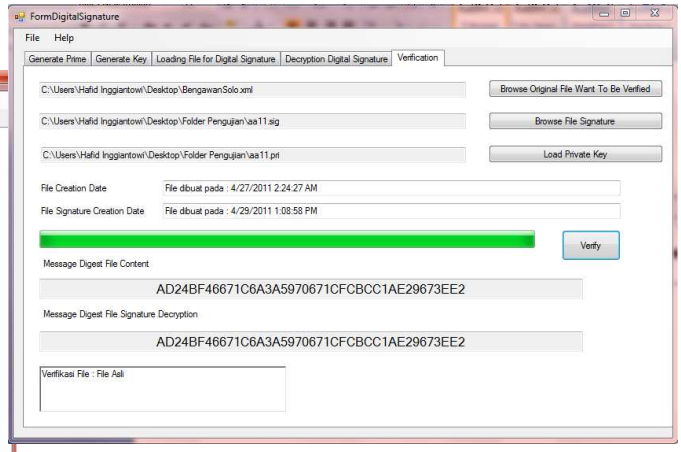


Gambar 6 Antarmuka pembuatan tanda tangan digital

Message digest dari file dihitung terlebih dahulu, kemudian hasil daripada perhitungan *message digest* ini dienkripsi dengan menggunakan algoritma RSA. Oleh karenanya perlu kunci privat dan kunci publik dalam proses pembubuhan tanda tangan digital ini. Sedangkan perhitungan *hash* yang menghasilkan *message digest* menggunakan algoritma *hash* SHA1.

Setelah selesai membubuhkan tanda tangan, maka dapat dilakukan verifikasi untuk nantinya dimana file tanda tangan akan dienkripsi untuk menghasilkan *message digest*, dan kemudian *message digest* ini akan dibandingkan dengan *message digest* daripada file asli. Jika sama, maka dapat dipastikan bahwa hasil verifikasi tersebut memang merupakan file asli. Antarmuka untuk verifikasi dapat dilihat pada Gambar 6.

Perubahan pada file MusicXML sedikit apapun akan mengubah *message digest* sehingga file dapat diperiksa integritasnya. Penggubah daripada partitur tersebut juga harus memiliki file asli daripada partitur MusicXML, file tanda tangan digital yang pernah dibuat, serta kunci privat, untuk dapat memverifikasi dan mengklaim bahwa file tersebut benar adalah file asli buatannya.



Gambar 7 Antarmuka verifikasi

Untuk program ini, sebaiknya tanda tangan digital tidak dibubuhkan langsung pada bagian di bawah atau di atas di dalam isi file karena nantinya partitur ini tidak akan dapat dibaca oleh perangkat lunak penulis musik karena mendefinisikan sesuatu yang bukan merupakan elemen tag XML.

Sedangkan usulan kedua, adalah menggunakan tanda tangan digital XML sebagaimana yang dijelaskan pada Bab IV. Contoh daripada tanda tangan digital XML yang akan dapat dihasilkan dapat dilihat sebagai berikut.

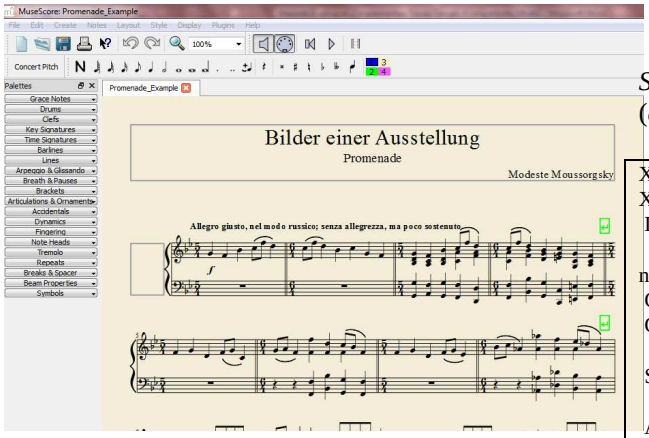
```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
  <CanonicalizationMethod
   Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
  <SignatureMethod
   Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
  <Reference URI="">
   <Transforms>
    <Transform
     Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
   </Transforms>
   <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
   <DigestValue>tVicGh6V+8cHbVYFIU91o5+L3OQ=</DigestValue>
  </Reference>
 </SignedInfo>
 <SignatureValue>
  dJDHiGQMaKN8iPuWApAL57eVnxz2BQtyujwfPSgE7HyKoxYtoRB97ocxZ
  8ZU440wHtE39ZwRGIjvwor3WfURxnIgnI1CChMXXwoGpHH//Zc0z4ejaz

DuCNEq4Mm4OUVTiEVuwcWAOMkfDHaM82awYQiOGcwMbZe38UX0oPJ2
DOE=
```

```
 </SignatureValue>
 <KeyInfo>
  <X509Data>
   <X509SubjectName>
    CN=My Name,O=Test Certificates Inc.,C=US
   </X509SubjectName>
   <X509Certificate>
    MIIB9zCCAWCgAwIBAgIERZwdkzANBgkqhkiG9w0BAQUFAD
BAMQswCQYD
    VQQGEwJVUzEfMB0GA1UEChMWVGVzdCBDZXJ0aWZpY2F0Z
XMgSW5jLjEQ
MA4GA1UEAxMHTXkgTmFtZTAeFw0wNzAxMDMyMTE4MTFaFw0zMTA4
MjUy
    ...
   </X509Certificate>
  </X509Data>
 </KeyInfo>
</Signature>
```

Gambar 8Tanda Tangan Digital XML

Pada usulan kedua ini, proses ini juga dapat dibuat pada suatu *add-in* misalnya pada perangkat lunak penulis musik yang dapat digunakan untuk menyimpan ke dalam format MusicXML. Contoh perangkat lunak penulis musik tersebut antara lain seperti Sibelius, Finale, Musescore, dan lain sebagainya. Contoh tampilan perangkat lunak penulis musik dapat dilihat pada Gambar 9. Adapun *add-in* dapat ditambahkan di bagian sebelah kanan menu Help ataupun pada bagian menu lainnya yang diinginkan. *Add-in* tersebut dibuat mengimplementasikan penandatanganan digital dengan tanda tangan digital XML.



Gambar 9 Perangkat lunak penulis musik

Alternatif lain lagi adalah tanda tangan digital XML ini dapat secara otomatis dibangkitkan langsung saat menuliskan MusicXML tersebut. Dengan kata lain, hal ini menjadi fokus penelitian daripada pengembangan standar musik MusicXML kembali sebagai standar musik yang telah digunakan secara luas di dunia.

Untuk keperluan keamanan lebih lanjut, misalkan tidak diinginkan partitur tersebut dapat dengan mudah dibaca oleh orang yang tidak berhak, partitur MusicXML ini juga dapat dienkripsi pada bagian elemen tag <*note*>-nya sehingga partitur yang dihasilkan hasil enkripsi merupakan partitur yang berbeda dengan partitur aslinya.

Oleh karena itu perlu pemrosesan pembacaan (*parsing*) nilai-nilai XML terutama pada bagian <note>, yang kemudian dienkripsi menjadi nada lain. Algoritma kriptografi yang memungkinkan untuk mengenkripsi nada yang dibaca menjadi nada lain adalah algoritma kriptografi klasik cipher substitusi. Namun, hal ini juga memiliki kompleksitas dalam implementasi, karena pada bagian nada, ia juga mendefinisikan elemen <*alter*> yaitu nilai kres atau mol yang dimiliki nada tersebut. Akibatnya, nada tidak dapat ditransformasi menjadi sembarang nilai daripada C, D, E, F, G, A, atau B, karena harus dapat dipastikan nada hasil enkripsi bukanlah nada yang jika memiliki kres atau mol adalah nada berikutnya. Contohnya seperti E dan B. Dan juga, algoritma kriptografi klasik seperti ini rawan dipecahkan dengan kriptanalisis.

IV. PENGUJIAN IMPLEMENTASI TANDA TANGAN DIGITAL XML PADA PARTITUR MUSICXML

Bagian ini akan menjelaskan hasil pengujian implementasi pembuatan tanda tangan digital. Pada Java contohnya, terdapat *Digital Signature XML API* yang dapat digunakan untuk membubuhkan tanda tangan digital yang dispesifikasikan pada :

- javax.xml.crypto
- javax.xml.crypto.dsig
- javax.xml.crypto.dsig.keyinfo
- javax.xml.crypto.dsig.spec
- javax.xml.crypto.dom
- javax.xml.crypto.dsig.dom

Source code untuk membuat tanda tangan XML terpisah (*detached signature*) dapat dilihat pada Gambar 10.

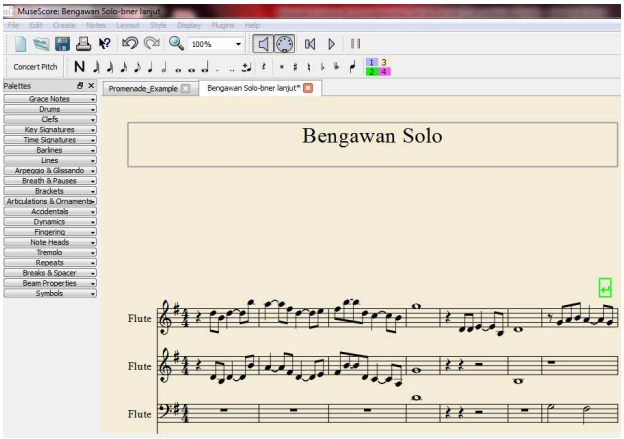
```
XMLSignatureFactory fac =
XMLSignatureFactory.getInstance("DOM");
 DigestMethod digestMethod =
     fac.newDigestMethod("http://www.w3.org/2000/09/xmldsig#sha1",
null);
 C14NMethodParameterSpec spec = null;
 CanonicalizationMethod cm = fac.newCanonicalizationMethod(
     "http://www.w3.org/2001/10/xml-exc-c14n#",spec);
 SignatureMethod sm = fac.newSignatureMethod(
     "http://www.w3.org/2000/09/xmldsig#rsa-sha1",null);
 ArrayList transformList = new ArrayList();
 TransformParameterSpec transformSpec = null;
 Transform envTransform =
fac.newTransform("http://www.w3.org/2001/10/xml-exc-
     c14n#",transformSpec);
 Transform exc14nTransform = fac.newTransform(
     "http://www.w3.org/2000/09/xmldsig#enveloped-
signature",transformSpec);
transformList.add(envTransform);
transformList.add(exc14nTransform);
Reference ref =
fac.newReference("",digestMethod,transformList,null,null);
ArrayList refList = new ArrayList();
refList.add(ref);
SignedInfo signedInfo =fac.newSignedInfo(cm,sm,refList);
```

Gambar 10 Pembuatan tanda tangan diselipkan (enveloped signature)

Setelah melakukan pengujian pembuatan tanda tangan

digital XML yang kemudian diselipkan pada MusicXML, didapatkan bahwa tanda tangan digital XML yang telah dispesifikasikan pada *XML-Signature Syntax and Processing Specification* (XML DSIG) ini telah didukung dengan baik oleh perangkat lunak penulis musik saat ini. Partitur berisi susunan nada-nada masih dapat dibaca dan dikembalikan tampilannya.

Percobaan dilakukan dengan menuliskan partitur musik Bengawan Solo yang dapat dilihat sekilas pada Gambar 10. Tampilan partitur setelah diselipkan tanda tangan digital masih tetap serupa dengan yang ditampilkan gambar tersebut. Gambaran isi partitur musik MusicXML yang telah dibubuhkan tanda tangan digital dapat dilihat pada bagian Lampiran.



Gambar 11 Bengawan Solo

Proses validasi dapat dilakukan dan didefinisikan pada *source code* pada Gambar 12 berikut.

```
public boolean validate(Element signature){
  DOMValidateContext validationContext = new
DOMValidateContext(new KeySelectorImpl(), signature);
  XMLSignatureFactory signatureFactory =
XMLSignatureFactory.getInstance("DOM");
  XMLSignature signature =
signatureFactory.unmarshalXMLSignature(validationContext);
  validationContext.setURIDereferencer(new URIResolverImpl());
  boolean validMessage  = signature.validate(validationContext);
     if(validMessage){
        System.out.println("Signature Validation passed");
     }else{
        System.out.println("Signature Validation Failed");
     }
  return validMessage;
}
```

Gambar 12Validasi Tanda Tangan Digital XML

V. KESIMPULAN

Partitur musik dengan format MusicXML dapat dibubuhkan tanda tangan digital. Dengan demikian, tanda tangan digital dapat menjadi metode pengamanan untuk pengembangan format tersebut. Tanda tangan digital pada MusicXML dapat digunakan untuk mencegah terjadinya klaim kepemilikan partitur oleh seseorang.

Masing-masing metode usulan memiliki kelebihan dan kekurangan. Untuk tanda tangan digital non XML, tanda tangan dengan jenis ini tidak dapat disisipkan langsung pada file dan harus dibuat merupakan tanda tangan digital yang terpisah. Hal ini dikarenakan pembacaan pada partitur penulis musik akan membaca tanda tangan digital yang bukan merupakan elemen tag XML. Sedangkan, untuk pembuatan tanda tangan digital XML, pembuatan tanda tangan dengan jenis ini memungkinkan untuk menyisipkan tanda tangan dalam file MusicXML dan juga pembuatan tanda tangan digital yang terpisah. Penyisipan tanda tangan XML pada file MusicXML tidak akan mempengaruhi pembacaan file MusicXML sebagai tulisan notasi not balok partitur pada perangkat lunak penulis musik. Namun, pembuatan tanda tangan digital XML memiliki beberapa kekurangan, yaitu kompleksitas dalam implementasinya dimana terdapat fungsi *canonicalization*. Proses *canonicalization* membuat proses penandatanganan menjadi lebih rumit karena perubahan satu byte saja pada pesan awal dapat mengakibatkan perubahan besar pada tanda tangan digital yang akan digunakan.

PUSTAKA

[1] *An Introduction to XML Digital Signatures*. http://www.xml.com/pub/a/2001/08/08/xmldsig.html

[2] *Ding, Y. MusicXML : An Internet Friendly Format For Sheet Music*. Diakses April 2011, http://www2.cs.uregina.ca/~gerhard/courses/Audio/MusicXML.ppt.pdf

[3] *Digital signature (electronic signature).* Diakses Mei 2011, Searchsecurity.com:http://searchsecurity.techtarget.com/definition/digital-signature

[4] *Java XML Digital Signatures.* Diakses Mei 2011, Oracle : Sun Developer Network (SDN): http://java.sun.com/developer/technicalArticles/xml/dig_signatures/

[5] *MusicXML : An Internet Friendly Format For Sheet Music*.Diakses April 2011, http://michaelgood.info/publications/music/musicxml-an-internet-friendly-format-for-sheet-music/

[6] *Programming with the Java XML Digital Signature API.* Diakses Mei 2011, Oracle : Sun Developer Network (SDN): http://java.sun.com/developer/technicalArticles/xml/dig_signature_api/

[7] *Munir, Rinaldi*. *Tanda Tangan Digital.* Diakses Mei 2011, http://www.informatika.org/~rinaldi/Kriptografi/2010-2011/TandaTanganDigital.ppt

[8] *Rivest, R.L., Shamir, A. , Adleman, L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems.* Diakses Mei 2011. http://people.csail.mit.edu/rivest/Rsapaper.pdf

[9] *Secure Hash Standard.* Federal Information Processing Standards Publication 180-2 (+ Change Notice to include SHA-224). Diakses Mei 2011. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

[10] *XML-Signature Syntax and Processing : W3C Recommendation 12 Feb 2002*. Diakses Mei 2011. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 8 Mei 2011

Hafid Inggiantowi

LAMPIRAN

```
?xml version="1.0" encoding="UTF-8"?>
   <!DOCTYPE score-partwise PUBLIC "-//Recordare//DTD
MusicXML 2.0 Partwise//EN"
"http://www.musicxml.org/dtds/partwise.dtd">
   <score-partwise>
    <identification>
     <encoding>
      <software>MuseScore 1.0</software>
      <encoding-date>2011-05-04</encoding-date>
      </encoding>
     </identification>
    <defaults>
   ……
     </defaults>
    <credit page="1">
   ……
         </credit>
    <part-list>
     <score-part id="P1">
      <part-name>Flute</part-name>
      <part-abbreviation>Fl.</part-abbreviation>
      <score-instrument id="P1-I3">
       <instrument-name>Flute</instrument-name>
       </score-instrument>
      <midi-instrument id="P1-I3">
       <midi-channel>1</midi-channel>
       <midi-program>74</midi-program>
       </midi-instrument>
      </score-part>
     <score-part id="P2">
      ……..
      </score-part>
     ……..
    </part-list>
    <part id="P1">
     <measure number="1" width="223.24">
      <print>
       <system-layout>
        …….
        </system-layout>
       </print>
      <attributes>
       <divisions>2</divisions>
       <key>
        <fifths>1</fifths>
        <mode>major</mode>
        </key>
       <time>
        <beats>4</beats>
        <beat-type>4</beat-type>
        </time>
       <clef>
        <sign>G</sign>
        <line>2</line>
        </clef>
       </attributes>
      <note>
       <rest/>
       <duration>2</duration>
       <voice>1</voice>
       <type>quarter</type>
       </note>
      <note default-x="115.16" default-y="-10.00">
       <pitch>
        <step>D</step>
        <octave>5</octave>
```

```
        </pitch>
       <duration>1</duration>
       <voice>1</voice>
       <type>eighth</type>
       <stem>down</stem>
       <beam number="1">begin</beam>
       </note>
      <note default-x="133.27" default-y="-20.00">
       ……
       </note>
      ……

      </measure>
   ……..

   </part>
         <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="">
      <Transforms>
       <Transform
        Algorithm="http://www.w3.org/2000/09/xmldsig#
   enveloped-signature"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/
   xmldsig#sha1"/>
      <DigestValue>tVicGh6V+8cHbVYFIU91o5+L3OQ=
   </DigestValue>
     </Reference>
    </SignedInfo>
    <SignatureValue>
     dJDHiGQMaKN8iPuWApAL57eVnxz2BQtyuj
   wfPSgE7HyKoxYtoRB97ocxZ
     8ZU440wHtE39ZwRGIjvwor3WfURxnIgnI1CC
   hMXXwoGpHH//Zc0z4ejaz
     DuCNEq4Mm4OUVTiEVuwcWAOMkfDHaM82aw
   YQiOGcwMbZe38UX0oPJ2DOE=
    </SignatureValue>
    <KeyInfo>
     <X509Data>
      <X509SubjectName>
       CN=My Name,O=Test Certificates Inc.,C=US
       </X509SubjectName>
      <X509Certificate>
       MIIB9zCCAWCgAwIBAgIERZwdkzANBgkqhki
   G9w0BAQUFADBAMQswCQYD
      VQQGEwJVUzEfMB0GA1UEChMWVGVzdCBD
   ZXJ0aWZpY2F0ZXMgSW5jLjEQ
      MA4GA1UEAxMHTXkgTmFtZTAeFw0wNzAxMD
   MyMTE4MTFaFw0zMTA4MjUy
      ...
      </X509Certificate>
     </X509Data>
    </KeyInfo>
   </Signature>
    </score-partwise>
```