IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727 Volume 5, Issue 4 (Sep-Oct. 2012), PP 01-04
www.iosrjournals.org

A novel approach for Multi-Tier security for XML based documents

Bimlendu Prasad Verma[1], Shiv Kumar[2], Prashant Sharma[3]
[1](Faculty of Engineering and Technology, Mewar University, India)
[2](Faculty of Engineering and Technology, Mewar University, India)
[3](J.T. Mahajan College of Engineering, North Maharashtra University, India)

Abstract: *Recently all the documents formats are being shifted from proprietary formats to the XML based standard formats. One of the key issues associated with any XML based document is security. Most of the approaches of security focus towards securing the access to the data rather than securing the data itself. So once the data/ document are out of their 'secured environment', they become completely open. However the data need to be secured in respect of confidentiality, integrity, authenticity and non-reproduction.*

Here we present an approach to achieve the Multi-Tier security that deals with providing integrity, non repudiation and different confidentiality levels for different users of the document. With this approach different users get to see only the allowed sections / sub sections of the XML based document.

Keywords - *Access control, Document security, Multi Tier Security, XML Security*

I. INTRODUCTION

Recently all the documents formats are being shifted from proprietary formats to the XML based standard formats. One of the key issues associated with any XML based document is security. Most of the approaches of security focus towards securing the access to the data rather than securing the data itself. So once the data/ document are out of their 'secured environment', they become completely open. However the data need to be secured in respect of confidentiality, integrity, authenticity and non-reproduction.

Security is essential in order to share the documents out of the 'secured environment'. The acceptance of XML is growing and so is the need of having XML security. The XML Security standards define XML based rules in order to meet security requirements.

The XML Security standards consist of the following:

- XML Digital Signature – This standard deals with the integrity and signing the XML document.
- XML Key Management (XKMS) – This deals with the public-private key registration and validation
- XML Encryption - This standard deals with the encryption and decryption of the XML based document for confidentiality.
- Security Assertion Markup Language (SAML) – This deals with conveying of authentication, authorization and attribute assertions.
- XML Access Control Markup Language (XACML) – This deals with the defining access control rules for the different part of the XML document.

Major use cases include securing Web Services (WS-Security) and Digital Rights Management (eXtensible Rights Markup Language 2.0 - XrML).

II. DOCUMENT SECURITY DETAILS

Electronic documents are fast replacing the paper based documents; be it electronic health records, photo albums, workflow systems, etc; however it is still far from real world needs on the aspects of security. Let's look at the current picture as far as document security goes:

2.1 Security – Current scenario

The term security encompasses all of the following:

Some of the prevailing document formats e.g. Adobe's PDF, SVG and Microsoft XDocs have either very limited or no built-in security implemented. Adobe PDF provides lock security – i.e. password for reading, writing and printing. However other formats lack on the security part.

What we propose is formats based on Open Standard XML complying to standards set by W3C and OASIS (ISO), with following security implemented:

- Single secure file that can be digitally signed
- Strong support for signatures, i.e. multiple and overlapping signatures
- Multiple encryptions for multiple types of access rights. Thus ensuring role based security

III. MULTI TIER SECURITY

3.1 Digital Signature

Normal digital signature guarantees three information security properties:

- Authentication: The signer is well identified by the private/public key relation.
- Non-repudiation: The signing party cannot later on deny performing the action, since the private key was used for encryption process. Note that if a symmetric key cryptography was used, the non-repudiation properties could not be guaranteed.
- Integrity: Since the signature itself is associated to the content to the message, any message alteration would make the signature invalid. This also implies that the signature cannot be copied from one message and applied to another.

The Single Digital Signature category is complete, but does not aim to replace all the utilizations of traditional written signature, since in many cases, more than one person are required to sign a legal document. Therefore Digital Multiple Signatures are very important. In everyday life, many legal documents require signatures from more than one party

For applying multiple and overlapping digital signatures, we could apply Sequential Multiple Signature In which we could sequentially sign the document many times. Refer figure 1.

3.2 Encryption

Since encryption granularity is XML node then we could encrypt and decrypt the desired part of full xml document according to roles. Refer figure 5.

This can be complimented using the implementation of Access control and Key Management system which will complete the security scenario.

IV. FIGURES AND TABLES

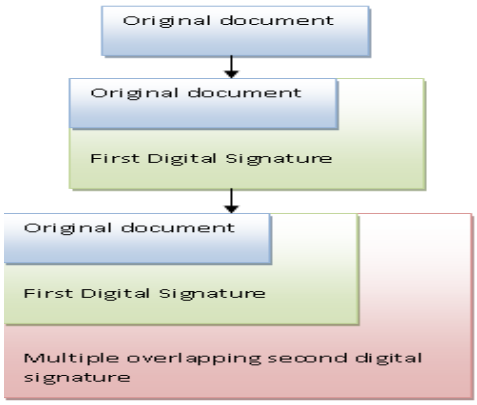

Fig. 1 Overlapping Digital Signatures.

```
<?xml version="1.0" encoding="UTF-8"?>
<office:document-meta
    xmlns:office="urn:oasis:names:tc:opendocument:xmlns:office:1.0"
    xmlns:xlink="http://www.w3.org/1999/xlink"
    xmlns:dc="http://purl.org/dc/elements/1.1/"
    xmlns:meta="urn:oasis:names:tc:opendocument:xmlns:meta:1.0"
    xmlns:ooo="http://openoffice.org/2004/office"
    xmlns:grddl="http://www.w3.org/2003/g/data-view#"
    office:version="1.2" grddl:transformation="http://docs.oasis-
    open.org/office/1.2/xslt/odf2rdf.xsl">
 <office:meta>
  <meta:creation-date>2009-04-16T11:32:02.64</meta:creation-date>
  <meta:editing-duration>PT00H00M47S</meta:editing-duration>
  <meta:editing-cycles>3</meta:editing-cycles>
  <meta:generator>OpenOffice.org/3.2$Win32
     OpenOffice.org_project/320m18$Build-9502</meta:generator>
  <dc:date>2012-08-01T12:33:20.57</dc:date>
  <meta:document-statistic meta:table-count="0" meta:image-count="0"
     meta:object-count="0" meta:page-count="1" meta:paragraph-count="1"
     meta:word-count="6" meta:character-count="27" />
  <dc:creator>Biml Verma</dc:creator>
  <meta:user-defined meta:name="Info 1" />
  <meta:user-defined meta:name="Info 2" />
  <meta:user-defined meta:name="Info 3" />
  <meta:user-defined meta:name="Info 4" />
    </office:meta>
    </office:document-meta>
```

Fig. 2 Original XML File (Meta.xml).

```
<office:document-meta
  xmlns:office="urn:oasis:names:tc:opendocument:xmlns:office:1.0"
  xmlns:grddl="http://www.w3.org/2003/g/data-view#"
  grddl:transformation="http://docs.oasis-
  open.org/office/1.2/xslt/odf2rdf.xsl" office:version="1.2"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:meta="urn:oasis:names:tc:opendocument:xmlns:meta:1.0"
  xmlns:ooo="http://openoffice.org/2004/office"
  xmlns:xlink="http://www.w3.org/1999/xlink">

<office:meta>
  <meta:creation-date>2009-04-16T11:32:02.64</meta:creation-date>
  <meta:editing-duration>PT00H00M47S</meta:editing-duration>
  <meta:editing-cycles>3</meta:editing-cycles>
  <meta:generator>OpenOffice.org/3.2$Win32
    OpenOffice.org_project/320m18$Build-9502</meta:generator>
  <dc:date>2012-08-01T12:33:20.57</dc:date>
  <meta:document-statistic meta:character-count="27" meta:image-count="0"
    meta:object-count="0" meta:page-count="1" meta:paragraph-count="1"
    meta:table-count="0" meta:word-count="6" />
  <dc:creator>Bimi Verma</dc:creator>
  <meta:user-defined meta:name="Info 1" />
  <meta:user-defined meta:name="Info 2" />
  <meta:user-defined meta:name="Info 3" />
  <meta:user-defined meta:name="Info 4" />
    </office:meta>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-
    xml-c14n-20010315#WithComments" />
  <ds:SignatureMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1" />
<ds:Reference URI="">
<ds:Transforms>
  <ds:Transform
    Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
    signature" />
    </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
    />
  <ds:DigestValue>Z6G0knRBjCQxagtKYH1hkuuxGp4=</ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>

    <ds:SignatureValue>Z7DwCinaed8AM8/8rjWfGoTAmuQ=</ds:SignatureVal
    ue>
    </ds:Signature>
    </office:document-meta>
```

Fig. 3 after applying first digital Signature (Meta.xml).

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>

<office:document-meta
    xmlns:office="urn:oasis:names:tc:opendocument:xmlns:office:1.0"
    xmlns:grddl="http://www.w3.org/2003/g/data-view#"
    grddl:transformation="http://docs.oasis-
    open.org/office/1.2/xslt/odf2rdf.xsl" office:version="1.2"
    xmlns:dc="http://purl.org/dc/elements/1.1/"
    xmlns:meta="urn:oasis:names:tc:opendocument:xmlns:meta:1.0"
    xmlns:ooo="http://openoffice.org/2004/office"
    xmlns:xlink="http://www.w3.org/1999/xlink">
<office:meta>
  <meta:creation-date>2009-04-16T11:32:02.64</meta:creation-date>
  <meta:editing-duration>PT00H00M47S</meta:editing-duration>
  <meta:editing-cycles>3</meta:editing-cycles>
  <meta:generator>OpenOffice.org/3.2$Win32
    OpenOffice.org_project/320m18$Build-9502</meta:generator>
  <dc:date>2012-08-01T12:33:20.57</dc:date>
  <meta:document-statistic meta:character-count="27" meta:image-count="0"
    meta:object-count="0" meta:page-count="1" meta:paragraph-count="1"
    meta:table-count="0" meta:word-count="6" />
  <dc:creator>Bimi Verma</dc:creator>
  <meta:user-defined meta:name="Info 1" />
  <meta:user-defined meta:name="Info 2" />
  <meta:user-defined meta:name="Info 3" />
  <meta:user-defined meta:name="Info 4" />
    </office:meta>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-
    xml-c14n-20010315#WithComments" />
  <ds:SignatureMethod
    Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1" />
<ds:Reference URI="">
<ds:Transforms>
  <ds:Transform
    Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
    signature" />
    </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
    />
  <ds:DigestValue>Z6G0knRBjCQxagtKYH1hkuuxGp4=</ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>

    <ds:SignatureValue>Z7DwCinaed8AM8/8rjWfGoTAmuQ=</ds:SignatureVal
    ue>
    </ds:Signature>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

Fig. 4 after applying second digital Signature (Meta.xml).

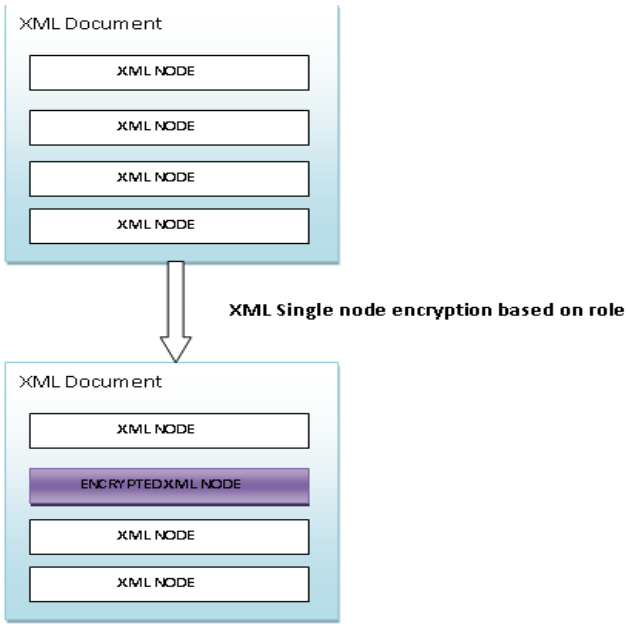

Fig. 5 Overlapping Digital Signatures

V. CONCLUSION

Electronic documents are fast replacing the paper based documents; be it electronic health records, photo albums, workflow systems, etc; however it is still far from real world needs on the aspects of security. Today's challenge is to make the electronic documents as relevant as their paper versions for their suitability for the legal documents such as contract papers, documents that record the workflow trails etc.

With the suggested approach it is possible to publish or hide the information based on roles, the overlapping signatures provide a way of authorizing the document by a set of people.

VI. Acknowledgements

We would like to thank Dr D.B. Ojha of Faculty of Engineering and Technology, Mewar University for encouraging and guiding us to write this paper.

REFERENCES

[1] Internet documentation at http://home.comcast.net/~fjhirsch/xml/xmlsec/starting-xml-security.html
[2] XML Security standards on W3 website http://www.w3.org/standards/xml/security
[3] XML Security information on W3 website www.w3.org/2004/Talks/0520-hh-xmlsec/.
[4] OASIS website for web service security (WSS) https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
[5] OASIS website for Web Services Security XrML-Based Rights Expression Token profile www.oasis-open.org%2Fcommittees%2Fwss%2Fdocuments%2FWSS-XrML-03-changes.pdf&ei=ZFYrUIuMC4KHrAe36oHICg&usg=AFQjCNFKOvbUYga98mruxq2d4KjBxzXEKg
[6] OASIS website on the XACML https://www.oasis-open.org/committees/xacml/
[7] XML Key Management Specifications on W3 website. www.w3.org/TR/xkms/
[8] OASIS website on the SAML https://www.oasis-open.org/committees/security/
[9] XML Key Management Specifications on W3 website. www.w3.org/TR/xkms/