

Signing messages

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2004-12/>

From: Martin Kulov (*kulov_at_bezbokluk.abv.bg*)

Date: 12/01/04

Date: Wed, 01 Dec 2004 04:52:39 -0800

So, message signatures are described in Signature\SignedInfo element.

And I am using WSE 2.0 SP2 Prerelease.

For example:

```
<SignedInfo>
  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1" />
  <Reference URI="#Id-9f6237be-83f3-4bb7-8e53-56c2a032b745">
    <Transforms>
      <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <DigestValue>ctf3qbSQ6hofrMjIrvsIaO1AaI=</DigestValue>
  </Reference>
  ..
  <SignatureValue>j7yVNKUvzh01hELvQk0fRFsXj+M=</SignatureValue>
  ..
</SignedInfo>
```

The receiver uses the canonicalization and digest methods to calculate reference digest. Is that correct?

My questions are:

Why do you need to have DigestValue in the envelope when the receiver can calculate it by himself using the canonicalization and digest methods?

What is this Transforms element for? I have not seen any description on it yet.

What is the difference between Canonicalization and Transform algorithm?

The SignatureValue contains signature based on all digest values. How it combines all digest in one value in order to sign that value the public key of the receiver? Using Canonicalization method may be?

microsoft.public.dotnet.framework.webservices.enhancements: Signing messages

What if an intermediate decides to change a header value that is signed? Then the whole signature value will be modified. Does not this break the security in some way? Is the signature gets recreated automatically when a part that is signed gets modified?

I just saw that Reference element is marked as obsolete. What is going to replace it?

Martin Kulov
www.codeattest.com