# Authoritative source on XML-sig

Asked 16 years, 4 months ago Modified 10 years, 3 months ago

Viewed 584 times

12

We have a question with regards to XML-sig and need detail about the optional elements as well as some of the canonicalization and transform stuff. We're writing a spec for a very small XML-syntax payload that will go into the metadata of media files and it needs to by cryptographically signed. Rather than re-invent the wheel, We thought we should use the XML-sig spec but I think most of it is overkill for what we need, and so we like to have more information/dialogue with people who know the details.

Specifically, do we need to care about either transforms or canonicalization if the XML is very basic with no tabs for formatting and is specific to our needs?

xml xml-signature

Share

Improve this question

Follow

edited Sep 10, 2014 at 20:14

Yurii

4,901 ● 7 ● 36 ● 44

asked Aug 7, 2008 at 15:33

chesterbestertester

123 ● 1 ● 6

## 3 Answers

Sorted by: Highest score (default)

0

✓

If the option exists to **not** do an XML signature and instead just to treat the XML as a byte stream and to sign that, do it. It will be easier to implement, easier to understand, more stable (no canonicalization, transform, policy, ...) and faster.

If you absolutely must have XML DSIG (sadly, some of us must), it is certainly possible these days but there are many, many caveats. You need good library support, with Java this is out of the box in JDK 1.6, I am not familiar with other platforms. You must test interoperability with the receiving end of your signed XML, especially if they are potentially on a different platform.

Be sure to read Why XML Security Is Broken, it basically covers all the ground regarding the horror that is XML Canonicalization and gives some pointers to some alternatives.

Share Improve this answer Follow

answered Aug 19, 2008 at 21:37

Boris Terzic
10.9k ● 8 ● 46 ● 60

---

0

Can you let us know that technology you are using as there are some intresting bits out there around this stuff and some short cuts... i.e. WSE2 is complex beast and something that I dont like getting wrong!

I dont like developers doing this and there are WSE2 accelorators out there like SSL Accelorates as the processing of encryption has a hugh cost best to take it out of process from the normal code and the development arena.

If this is an option for you - [Try look at this - ForumSystems]

Share Improve this answer Follow

answered Aug 13, 2008 at 7:52

littlegeek

---

0

If you need to sign XML in code, check [XMLBlackbox] which provides canonicalization and all other transformations for you. XMLBlackbox also supports XAdES.

Share Improve this answer Follow

answered Dec 20, 2008 at 10:39

Eugene Mayevski 'Callback

46k ● 8 ● 74 ● 122