

C++ Library Documentation

1. News - August 2003

Version 1.00 of the library has now been released. It features :

- the first stable release
- full implementation of all mandatory requirements of DSIG
- implementation of canonicalised XML
- implementation of exclusive-canonicalised XML
- implementation of XPath-filter
- FreeBSD, NetBSD and Cygwin builds

Version 1.00 is has been tested with Xerces-C v2.2 and the newly released Xalan-C v1.6. Xerces-C v2.3 is also supported. Note that versions of Xalan prior to v1.6 are not supported (due to the new changed location of include files).

2. Overview of the C++ Library

The C++ library is an implementation of the XML Digital Signature specification. It is designed to be easily ported to new platforms, and has been tested on Solaris, Linux, FreeBSD, NetBSD and Windows.

The library makes use of the Apache XML project's Xerces-C XML Parser and Xalan-C XSLT processor. The latter is used for processing XPath and XSLT transforms. The use of Xalan-C is optional, but without it, XPath and XSLT transformations cannot be performed.

In addition, the library currently uses OpenSSL to provide cryptographic functionality. The cryptographic interface is implemented via a thin wrapper layer, and a development version of an implementation for the Windows Cryptographic API has also been implemented.

3. Old News

3.1. May 2003

Beta 0.2 has been released. It covers :

- some minor bug-fixes in the code and the UNIX build system
- a first cut at a Windows Crypto API provider interface

- methods to extract information from signature objects; and
- updates to tools to allow (and demonstrate) use of Windows CAPI and new extraction methods

Beta 0.2 is has been tested with Xerces-C v2.2 and the newly released Xalan-C v1.5.

3.2. February 2003

The C++ library has now been fully transferred into the Apache XML project. It was previously hosted on SourceForge.

The first release under Apache is 0.10. This is a Beta release, with fairly complete documentation, and a stable code base. It fully validates the various interop documents held in the xml-security CVS, with the exception of those related to :

- MD5 Digests (to be added in next point release)
- XPath Filter (to be added in next point release)
- XML Encryption (to be added post 1.00 release)