Release Information

1. Changes

This section describes the changes that have occurred between the various releases of the library

1.1. Current Release - Beta 0.20

Includes a number of bug-fixes and a first cut at a provider for the Windows Crypto API.

1.2. Changes from 0.10-0.10

The current release of the xml-security-c library is a beta of the XML Digital Signature code, and is the first version of the library produced within Apache's XML project.

Previous versions were created within Sourceforge as the xml-security-c project at that site.

1.3. Changes from 0.03-0.10

The following changes occurred between versions 0.03 and 0.10 :

- A *threadTest* tool, which is primarily used to show how multiple threads can access the library under Windows
- Windows and UNIX URI Resolvers, based on the Xerces resolver, but which can handle HTTP re-directs
- Completed a basic level of API documentation
- Reviewed library to ensure usage of UTF-16 internally
- Closed a number of memory-leaks caused by exceptions being thrown

1.4. Changes from 0.02-0.03

The following changes occurred between 0.02->0.03

- A *txfmout* tool to output the transformed references
- Updates to *templatesign* to support KeyInfo elements and RSA signatures
- Library support for RSA signatures
- API support form manipulating KeyInfo elements

- Pluggable KeyInfo Resolvers (to allow an application to supply an object that will resolve a given KeyInfo to a key)
- Pluggable URI resolvers
- API support for creating references and transformations
- Re-written Makefiles for *NIX
- Improved API docs
- Envelope Transform that no longer uses XPath transforms (much quicker)
- Uses new Xerces DOMNode objects - has made for significant speed improvements

1.5. Changes from 0.01-0.02

- Signing functionality
- Update C14n canonicalisation
- Exclusive Canonicalisation
- Basic ability to create a signature via the API (rather than just from an XML template file
- SHA-1 HMAC support
- Basic Documentation of core API
- A *templatesign* tool

2. Future Release Plans

The current plans are to stablise the beta code and provide a sound core library for digital signing. Now that the code is at 0.20, some further additions will be made to the digital signature support, and a 1.00 release will be made when digital signature support is fairly complete.

XML Encryption will be added post 1.00

The majority of activity from now to 1.00 will concentrate on:

- Fixing bugs and memory leaks
- Ensure API is reasonably consistant
- Improvements in the API for manipulating a signature in memory
- Support for KeyInfo elements not currently implemented (PGP and SPKI)
- NetBSD/FreeBSD builds
- Install capability in make files

3. Beyond a stable release

A number of items are planned for after the 1.0 major release.

- XML Encryption Support
- Implementation of a core set of encryption primitives to allow decoupling from OpenSSL

for "light" applications
- Improved *KeyInfo* resolver interface leading to...
- XKMS client support
- Implementation of libgcrypt as a crypto provider
- Support for PGP/GPG signatures (using libgcrypt and gpgme)
- Bring the API in-line with JCP 105 (if appropriate)
- Eventually (the GRAND PLAN) an XKMS server implementation