Index

Welcome to Apache Santuario™

The Project

The **Apache Santuario™** project is aimed at providing implementation of the primary security standards for XML:

- XML-Signature Syntax and Processing
- XML Encryption Syntax and Processing.

Two libraries are currently available.

- Apache XML Security for Java: This library includes the standard JSR-105 (Java XML Digital Signature) API, a mature DOM-based implementation of both XML Signature and XML Encryption, as well as a more recent StAX-based (streaming) XML Signature and XML Encryption implementation.
- Apache XML Security for C++: This library includes a mature Digital Signature and Encryption implementation using a proprietary C++ API on top of the Xerces-C XML Parser's DOM API. It includes a pluggable cryptographic layer, but support for alternatives to OpenSSL are less complete and less mature.

However, the C++ library is now frozen and will be retired from Apache in the near future, per the news item below.

News

March 2024

After discussion with the Santuario PMC, it has been decided to address the long term lack of support for the C++ library by formally retiring the code here at Apache. The Java code of course remains well supported and will continue to be developed.

As of now, the C++ code is frozen here. The current sole maintainer will be transferring the source code to the Shibboleth Project and it will be maintained by that team for some period of time because it is a dependency of that software, but it will not be supported for any third-party use. It is estimated that the code will be fully retired some time before 2030. The code will be publically hosted and accessible after the transition, and the license is not changing.

Once the code transition occurs, which may not be for some time yet, we will update more of the site as is appropriate to reflect the transition. In the event a significant issue arises with the library prior to the transition, we will endeavor to address it here.

February 2024

Version 4.0.2 and 3.0.4 of the Apache XML Security for Java library have been released. They contain a new feature to support Key Agreement using ECDH-ES.

November 2023

Version 4.0.1 of the Apache XML Security for Java library has been released, containing a bug fix (SANTUARIO-609 - Remove call to Signature. getProvider() in debug log)

October 2023

Versions 4.0.0, 3.0.3, 2.3.4 and 2.2.6 of the Apache XML Security for Java library have been released. A security advisory has been fixed in these releases:

- CVE-2023-44483: Apache Santuario: Private Key disclosure in debug-log output

Please see the Security Advisories page for more information.

September 2023

Version 4.0.0-M1 of the Apache XML Security for Java library has been released. This is a preview release of the forthcoming 4.0.0 release which is made available for testing, it should not be used in production. The main changes are:

- Java 11 requirement
- Removing SLF4J and using System.Logger
- AutoCloseable for several types

August 2023

Version 2.2.5 of the Apache XML Security for Java library has been released. It contains some dependency updates to fix CVE reports.

March 2023

Versions 3.0.2 and 2.3.3 of the Apache XML Security for Java library have been released. Support for the EdDSA has been added as part of these releases.

November 2021

Version 2.0.4 of the Apache XML Security for C++ library has been released. This release fixes a regression in 2.0.3 allowing the code to build on pre-1.1 OpenSSL versions.

Older News

See here for old news.