

# java\_index

## Apache XML Security for Java

### Overview

The Apache XML Security for Java library supports [XML-Signature Syntax and Processing, W3C Recommendation 12 February 2002](#) and [XML Encryption Syntax and Processing, W3C Recommendation 10 December 2002](#).

There are a number of different options open to the developer using the library. For XML Signature, three different approaches are available:

- The JSR-105 API: The standard Java XML Digital Signature API. This uses a DOM (in-memory) implementation under-the-hood.
- The Apache Santuario Java DOM API: The older DOM API which pre-dates JSR-105.
- The Apache Santuario Java StAX API: The newer StAX-based (streaming) API which uses far less memory for large XML trees than the DOM approach.

For XML Encryption, two different approaches are available:

- The Apache Santuario Java DOM API: A DOM API for XML Encryption.
- The Apache Santuario Java StAX API: The newer StAX-based (streaming) API which uses far less memory for large XML trees than the DOM approach.

The StAX-based (streaming) functionality is only available as of the 2.0.0 release. Please see the [Streaming XML Security](#) page for more information about how to use this approach.

### News

#### 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.

### Old News

See [here](#) for older news.