java_1_5_7_release_notes

Apache XML Security for Java 1.5.7 release notes

Bug

- [SANTUARIO-307] - utf8 encode is broken
- [SANTUARIO-350] - Unmarshalling from existing elements doesn't enforce syntax & semantic requirements
- [SANTUARIO-379] - Signing XML with SHA1 with DSA throws exception when key is larger than 1024
- [SANTUARIO-383] - NPE in DOMXMLSignature
- [SANTUARIO-391] - Support for Signature Algorithm RSA with SHA-224
- [SANTUARIO-393] - Performance regression as signature data is not buffered

Improvement

- [SANTUARIO-375] - Canonicalizer.ALGO_ID_C14N_PHYSICAL's initialization
- [SANTUARIO-388] - Add support + testing for RIPE-MD160 digest algorithm
- [SANTUARIO-389] - Add support + testing for SHA-224 digest algorithm
- [SANTUARIO-392] - In XMLCipher support use of GCMParameterSpec for AES GCM modes