

OSCI-Bibliothek (JAVA) – Versionshistorie

Version	Datum	Änderungen gegenüber Vorversion
0.96 Beta	24.11.2003	./.
0.97 Beta	08.12.2003	Überarbeitung der Schnittstellen der Bibliothek (kleinere Ergänzungen, Entfernung der <code>DialogFinder</code> -Schnittstelle und der Archivierungsfunktionen durch die <code>OSCIDataSource</code> -Schnittstelle), div. Bugfixes
0.98 Beta	15.12.2003	Implementierung MIME-Parser, Überarbeitung Schemadefinition, AES-Einbindung, <code>StoreMessage</code> -Klasse hinzugefügt, div. Bugfixes
1.00	09.03.2004	Verbesserte Unterstützung des Sprachinterface, Unterstützung der <code>Progress</code> -Schnittstelle, Fehlerbehandlung verbessert, Dokumentation qualitätsgesichert, div. Bugfixes
1.01	02.04.2004	ID-Schreibweise in XML-Dokumenten korrigiert; bei paralleler Mehrfachsignatur mit identischem Zertifikat wird nun jede Signatur geprüft; kleinere Korrekturen vorgenommen
1.02	30.04.2004	Probleme bei Benutzung ohne Debug-Einstellung beseitigt
1.03	23.06.2004	Korrigenda vom 10.06.2004 zur OSCI-Spezifikation 1.2 eingearbeitet, <code>ContentPackageIInterface</code> erweitert, Zertifikatsreferenzen vereinheitlicht, Bugfixes, <code>ProcessCard</code> -Operationen erweitert
1.04	08.07.2004	Dialogeröffnung mit Test-Intermediär nur via <code>InitDialog</code> -Nachricht möglich, <code>FeedbackObject</code> -Klasse eingeführt, die Methode <code>ContentContainer.checkAllSignatures()</code> wirft nun bei Nichtvorhandensein einer Signatur eine Exception, <code>MediateDelivery</code> erlaubt nun auch Message-IDs ohne Subject (laut Spezifikation), Default bei <code>QualityOfTimeStamp</code> -Eigenschaften ist nun <code>plain</code>
1.1	06.12.2004	Diverse Bugfixes, z.B. ein Problem mit Attachments, die in verschachtelten Content-Containern referenziert werden, beseitigt. Laufzettelaufträge für mehrere Message-IDs erweitert. Diverse Anpassungen und Änderungen mit dem Ziel der Kompatibilität mit Apache-XML Implementierungen. Base64-Codierung der Attachments als Transfer-Encoding. Transport-Interface um Methode <code>newInstance()</code> erweitert (Thread-Sicherheit in „automatischen“ Clients)
1.1.1	14.07.2005	Das Schließen von HTTP-Streams wurde verbessert. Schließen der Input-Streams in <code>Content</code> wurde überarbeitet. Ein Problem beim Parsen von <code>ResponseToProcessDelivery</code> bei fehlendem Originator <code>o</code> . Addressee wurde beseitigt und das Lesen von SOAP-Error-Nachrichten (mit <code>StoreInputStreams</code>), die keine Schema-Definition enthalten, wurde verbessert. Es wurde ein Problem mit abgeleiteten Rollenklassen behoben. <code>Inspections</code> codieren die DNs nun XML-konform (nur für Intermediär). Es wird nur noch die Key-Usage <code>non-repudiation</code> gecheckt und nun auch die Key-Usage <code>digital signature</code> zugelassen. Kollisionen von Referenz-IDs (z.B. mehrere <code>author0 *</code>) durch importierte

Version	Datum	Änderungen gegenüber Vorversion
		Content-Container wurden beseitigt.
1.2	03.02.2006	<p>Es wurden zahlreiche Änderungen mit dem Ziel der Kompatibilität zu kommerziellen XML-Implementierungen vorgenommen. Hervorzuheben ist hier die Entfernung von Leerzeilen in dem Attachment MIME-Container.</p> <p>Es wurden Änderungen vorgenommen, um die Namespace-Präfixe variabel zu gestalten. Grenzen in der Realisierung haben sich durch XML-Signature ergeben, da ansonsten Signaturen unverschlüsselter Inhaltsdaten bei Änderungen der Präfixe ungültig würden.</p> <p>Temporäre Dateien werden nun beim Beenden der JRE gelöscht. Die Java-Bibliothek unterstützt nun den Längenparameter, der an die <code>getConnection</code>-Methode des Transport-Interfaces übergeben wird. Die Länge der Nachricht wird vorher berechnet.</p> <p>Die Base64-Codierung für den Transportumschlag und Attachments ist nun optional, bleibt jedoch Default. Diese Default-Belegung sollte nur bedacht geändert werden, da sich hieraus Inkompatibilitäten bei der Kommunikation mit vorherigen Versionen der OSCI-Bibliothek (und Intermediären) ergeben.</p> <p>Im <code>DialogHandler</code> können nun mehrere Default-Supplier, also mehrere Privatschlüssel, für die Entschlüsselung eingehender Nachrichten (und ggf. Signatur der Antworten) gesetzt werden.</p>
1.2.1	03.03.2006	Kleinere Probleme der Version 1.2 beseitigt (Längenberechnung verschlüsselter Nachrichten, Reihenfolge der Content-Container-/EncryptedData -Tags, Namespace-Deklarationen in zusätzlichen SOAP-Headern)
1.2.2	14.06.2006	Problem mit signierten verschachtelten Content-Containern, die Attachments enthalten, behoben. Verlust des Base64-Transformers der Inhaltsdatensignatur beim Laden gespeicherter Nachrichten beseitigt. Neue Methode zum Laden gespeicherter Nachrichten mit Prüfung der Nachrichtensignatur in der Klasse <code>StoredMessage</code> . Neue Methoden in der Klasse <code>OSCIMessage</code> zum Zugriff auf Content-Container und Content-Objekte anhand des <code>refID</code> -Attributs.
1.2.3	06.12.2006	Methode <code>SwapBuffer.setTmpDir(String)</code> zum Setzen des Verzeichnisses für temporäre Dateien hinzugefügt. Neue abstrakte Subklasse von <code>OSCIDataSource</code> (<code>OSCIDataSourceExt123</code>) zur Unterstützung der Verschlüsselung temporärer ggf. vertraulicher Inhaltsdaten.
1.2.4	27.02.2007	Zusätzliches Attribut <code>mimeHeaders</code> in der Attachment-Klasse für weitere Header-Einträge des umschließenden MIME-Boundary-Abschnitts
1.2.5	17.04.2007	Überarbeitung der Verwendung gesetzter Security-Provider (durchgängige Nutzung des Providers für alle kryptographischen Operationen außer der Zufallszahlenerzeugung). Kleinere Änderungen, z.B. Exception-Handling der XML-Parser.
1.2.6	05.09.2007	Begrenzung der Attachment-Größe auf 2 GB beseitigt. Problem mit IBM-JDK behoben. <code>Base64InputStream.available()</code> -

Version	Datum	Änderungen gegenüber Vorversion
		Methode implementiert. Kleinere Änderungen, z.B: Behandlung der Namespace-Deklaration von Signaturen beim Speichern von Nachrichten
1.3	12.2.2008	Erweiterung auf neue Hashalgorithmen gemäß Korrigenda der OSCI 1.2 Transport Spezifikation v. 11.2.2008. Hierzu Erweiterung des Signer-Interfaces um die Methode <code>getAlgorithm()</code> . Übergangsweise wird SHA-1 weiter unterstützt. Zur Kontrolle der Signaturstärke empfangener Signaturen zwei neue Methoden <code>OSCIMessage.hasWeakSignature(Date)</code> und <code>ContentContainer.hasWeakSignature(Role, Date)</code>
1.3.1	15.10.2008	Workaround f. Bug #6219755 im JDK 1.5 (Ansammlung von Threads) im Serverbetrieb. Methode <code>ContentContainer.getSignatures()</code> zum Ermitteln der Signatur- und Hashalgorithmen von Inhaltsdatensignaturen. Neues Attribut <code>OSCIMessage</code> in <code>OSCIErrorException</code> . Problem mit ungültigen Nachrichtensignaturen bei seriell verschlüsselten Inhaltsdaten behoben. Default-Algorithmus für symmetrische Verschlüsselung auf AES-256 umgestellt.
1.3.2	03.06.2010	Anpassung an Ablauf des Hashalgorithmus RIPEMD-160 zum 31.12.2010. Die Prüfmethode <code>hasWeakSignature(...)</code> liefern bei Prüfung ohne Datumsangabe für diesen Algorithmus <code>true</code>. Methoden für frei formulierte Feedback-Texte in synchronen Szenarien auf Empfängerseite. Kleinere Überarbeitungen.
1.4	10.11.2010	Vorbereitung für die Aufnahme von Signaturzeitpunkten in Inhaltsdatensignaturen (rudimentäre XAdES-Unterstützung). Diverse kleinere Überarbeitungen.
1.5	19.11.2010	Unterstützung elliptischer Kurven als Signaturalgorithmen (Korrigenda v. Oktober 2011). Kleinere Überarbeitungen.
1.6	16.04.2014	Unterstützung von OAEP-Algorithmen für Verschlüsselung und Signaturen gemäß Korrigenda der OSCI 1.2 Transport Spezifikation v. 20.2.2014. Implementierungen der Schnittstelle <code>de.osci.oscil2.ext.interfaces.crypto.Decrypter</code> müssen für die Verwendung von RSAES-OAEP-ENCRYPT um eine entsprechende Methode erweitert werden.
1.6.1	30.09.2015	Bug-Fixes in der OSCI-Bibliothek, da in bestimmten Situationen OSCI-Fehlermeldungen auf Nachrichtenebene ausgegeben wurden (OSCI_9300).
1.7	22.02.2017	Umstellung auf die neuere Version des BouncyCastle-Security-Providers 1.55 und Einbinden von neueren Testzertifikaten. Es wird unterbunden, dass für mehrere Inhaltsdaten gleiche Referenz-IDs verwendet werden oder nachträglich dahingehend geändert werden können. Einbindung der SHA3-Hash-Algorithmen Sicherheits-Update: Anpassungen an den Prüfungen von XML-Dokumenten und Aufrufen des verwendeten XML-Parsers. Für die Verwendung des CBC-Modus sind serverseitig zusätzliche

Version	Datum	Änderungen gegenüber Vorversion
		Sicherheitsmaßnahmen nötig. Daher wurde ein neuer Modus (GCM) hinzugefügt, der langfristig den CBC-Modus ablösen wird.
1.7.1	03.03.2017	Die Überprüfung von mehrfach verwendeten Referenz-IDs kann durch das Setzen einer System Property gesteuert werden. Bug-Fix , da es unter bestimmten Umständen einen Fehler beim Abholen von OSCI-1.2-Nachrichten gab.
1.8	08.08.2017	Es wurden verschiedene Änderungen vorgenommen, um die paketierte Übertragung von Nachrichten, die in der Erweiterung der OSCI-Spezifikation bzgl. effizienter Datenübertragung beschrieben ist, zu ermöglichen. Es gibt Methoden um die zusätzlichen Header, wie die <code>FeatureDescription</code> und die <code>ChunkInformation</code> , zu erstellen. Außerdem gibt es Methoden um die neuen Nachrichtentypen <code>PartialStoreDelivery</code> und <code>PartialFetchDelivery</code> aufzubauen sowie die Response Nachrichten zu verarbeiten. Die Aufteilung einer großen Nachricht in Pakete wird an einem Beispiel demonstriert.