OSCI-Bibliothek (JAVA) – Versionshistory

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 DialogFinder-Schnittstelle und der Archivierungsfunktionen durch die OSCIDataSource-Schnittstelle), div. Bugfixes
0.98 Beta	15.12.2003	Implementierung MIME-Parser, Überarbeitung Schemadefinition, AES-Einbindung, StoreMessage-Klasse hinzugefügt, div. Bugfixes
1.00	09.03.2004	Verbesserte Unterstützung des Sprachinterface, Unterstützung der Progress-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, ContentPackageInterface erweitert, Zertifikatsreferenzen vereinheitlicht, Bugfixes, ProcessCard-Operationen erweitert
1.04	08.07.2004	Dialogeröffnung mit Testintermediär nur via InitDialog-Nachricht möglich, FeedbackObject-Klasse eingeführt, die Methode ContentContainer.checkAllSignatures() wirft nun bei Nichtvorhandensein einer Signatur eine Exception, MediateDelivery erlaubt nun auch MessageId ohne Subject (laut Spec), Default bei QualityOfTimeStamp-Eigenschaften ist nun „plain“
1.1	06.12.2004	Diverse Bugfixes, z.B. ein Problem mit Attachments, die in verschachtelten ContentContainern referenziert werden, beseitigt. Laufzettelabholaufträge 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 „newInstance()“ erweitert (Threadsicherheit in „automatischen“ Clients)
1.1.1	14.07.2005	Das Schließen von HTTP-Streams wurde verbessert. Schließen der InputStreams in Content wurde überarbeitet. Ein Problem beim Parsen von ResponseToProcessDelivery bei fehlendem Originator o. Addressee wurde beseitigt und das Lesen von SOAP-Error-Nachrichten (mit StoreInputStreams), die keine Schema-Definition enthalten, wurde verbessert. Es wurde ein Problem mit abgeleiteten Rollenklassen behoben. Inspections codieren die DNs nun XML-konform (nur für Intermediär). Es wird nur noch die keyusage non-repudiation gecheckt und nun auch die key usage 'digital signature' zugelassen. Kollisionen von Referenz-Ids (z.B. mehrere author0_*) durch importierte ContentContainer wurden beseitigt.
1.2	03.02.2006	Es wurden zahlreiche Änderungen mit dem Ziel der Kompatibiliät zu kommerziellen XML-Implementierungen vorgenommen. Hervorzuheben ist hier die Entfernung von Leerzeilen in dem Attachment MIME-Container. Es wurden Änderungen, um die Namespace-Präfixe variabel zu gestalten, vorgenommen. Grenzen in der Realisierung haben sich durch XML-Signature ergeben, da ansonsten Signaturen unverschlüsselter Inhaltsdaten bei Änderungen der Präfixe ungültig würden. Temporäre Dateien werden nun beim Beenden der JRE gelöscht.

		Die JAVA-Bibliothek unterstützt nun den Längenparameter, der an die getConnection-Methode des Transport-Interfaces übergeben wird. Die Länge der Nachricht wird vorher berechnet. 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. Im DialogHandler können nun mehrere Default-Supplier, also mehrere Privatschlüssel, für die Entschlüsselung eingehender Nachrichten (und ggf. Signatur der Antworten) gesetzt werden.
1.2.1	03.03.2006	Kleinere Probleme der Version 1.2 beseitigt (Längenberechnung verschlüsselter Nachrichten, Reihenfolge der ContentContainer-/EncryptedData –Tags, Namespace-Deklarationen in zusätzlichen SOAP-Headern)
1.2.2	14.06.2006	Problem mit signierten verschachtelten ContentContainern, 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 StoredMessage. Neue Methoden in der Klasse OSCIMessage zum Zugriff auf ContentContainer- und Content-Objekte anhand des refId-Attributs.
1.2.3	06.12.2006	Methode SwapBuffer.setTmpDir(String) zum Setzen des Verzeichnisses für temporäre Dateien hinzugefügt. Neue abstrakte Subklasse von OSCIDataSource (OSCIDataSourceExt123) zur Unterstützung der Verschlüsselung temporärer ggf. vertraulicher Inhaltsdaten.
1.2.4	27.02.2007	Zusätzliches Attribut „mimeHeaders“ in der Attachment-Klasse für weitere Headereinträge 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 Attachmentgröße auf 2 GB beseitigt. Problem mit IBM-JDK behoben. Base64InputStream.available()-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 getAlgorithm(). Übergangsweise wird SHA-1 weiter unterstützt. Zur Kontrolle der Signaturstärke empfangener Signaturen zwei neue Methoden OSCIMessage.hasWeakSignature(Date) und ContentContainer. hasWeakSignature(Role, Date)
1.3.1	15.10.2008	Workaround f. Bug #6219755 im JDK 1.5 (Ansammlung von Threads) im Serverbetrieb. Methode ContentContainer.getSignatures() zum Ermitteln der Signatur- und Hashalgorithmen von Inhaltsdatensignaturen. Neues Attribut „OSCIMessage“ in OSCIErrorException. 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 Prüfmethoden hasWeakSignature(...) liefern bei Prüfung ohne Datumsangabe für diesen Algorithmus „true“**. 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.