Aktuelle Hinweise zur OSCI 1.2 Transport Bibliothek in Java und .NET

Koordinierungsstelle für IT-Standards, November 2019

Die aktuelle Version 1.8.3 enthält Sicherheitsupdates der OSCI-Bibliothek. Die KoSIT empfiehlt, stets die aktuellste Version der Bibliothek zu verwenden.

- Meldung im CERT-Bund
- Sicherheitsempfehlungen zur OSCI Transport Bibliothek 1.8.3 (Java und .NET)

Die KoSIT empfiehlt aus Sicherheitsgründen den Einsatz von AES-GCM, maßgeblich sind jedoch die fachlichen Vorgaben. Die OSCI-Bibliothek wird in unterschiedlichen Einsatzszenarien mit individuellen Profilen verwendet. Die KoSIT empfiehlt daher die OSCI API-Funktionen zu verwenden, bei denen der zu verwendende Algorithmus explizit angegeben wird.

Für die Verwendung von AES-GCM ist Folgendes zu beachten:

1. **Für die Verschlüsselung der Fachnachricht (Inhaltsdaten) muss die Verwendung von AES-GCM explizit vorgegeben werden**, z.B. durch

   EncryptedDataOSCI(Constants.SYMMETRIC_CIPHER_ALGORITHM_AES256_GCM, contentContainer).

   Ein Aufruf der Art *EncryptedDataOSCI(contentContainer)* verschlüsselt nicht mit AES-GCM, da hierbei die Standardeinstellung (Default) der OSCI-Bibliothek verwendet wird. Diese ist in Version 1.8.3 aus fachlichen Gründen AES-CBC.

2. **Für die Verschlüsselung der Transportnachricht (Nutzdaten) verwendet die Version 1.8.3 automatisch AES-GCM, wenn beide Kommunikationspartner den Modus unterstützen, andernfalls wird AES-CBC verwendet.** Die KoSIT empfiehlt den Einsatz von AES-GCM. Falls aus fachlichen Gründen dennoch der Einsatz von AES-CBC erforderlich ist, kann dies entsprechend konfiguriert werden:
   - Kurzanleitung zur Festlegung von CBC als einzigem Modus in Java
   - Kurzanleitung zur Festlegung von CBC als einzigem Modus in .NET

RSA-OAEP wird von der OSCI-Bibliothek unterstützt.
Im Fall einer Fehlermeldung der Art „UnsupportedOperationException“ im Kontext RSA-OAEP ist zu prüfen, ob die Decrypterklasse angepasst wurde und eine zusätzliche Entschlüsselungsmethode mit der folgenden Signatur enthält:

public byte[] decrypt(byte[] data, String mgfAlgorithm, String digestAlgorithm) throws OSCICipherException, de.osci.osci12.common.OSCICancelledException

Eine Beispielimplementierung findet sich der Klasse de.osci.osci12.samples.impl.PKCS12Decrypter.

Bei der Version 1.8.3 der OSCI 1.2 Transport Bibliothek ist standardmäßig (default) die „Feature Description“ eingeschaltet.
Diese Einstellung ist für die meisten Anwendungssituationen völlig ausreichend und sollte möglichst beibehalten werden. Falls Sie die Feature Description nicht verwenden wollen, setzen Sie bitte zur Deaktivierung die folgenden beiden Schalter auf „false“:

DialogHandler.setSendFeatureDescription(false) und

de.osci.SendFeatureDescription=false

Außerdem muss folgendes leeres Feature gesetzt werden:

.setFeatureDescription(null)

Bitte gehen Sie zur Deaktivierung der Feature Description unbedingt wie angegeben vor, andernfalls kommt es bei aktivierter Transportsignatur zu einer ungültigen Signatur und damit zu einer entsprechenden Fehlermeldung beim Empfänger.

Handreichung für den zeitlichen Ablauf der Umstellung von AES-CBC auf AES-GCM

Für den Verschlüsselungsalgorithmus AES empfehlen sowohl das W3C als auch das BSI aus Sicherheitsgründen den Einsatz des Betriebsmodus GCM vorrangig vor dem CBC-Modus. Um einen geordneten Übergang von AES-CBC zu AES-GCM bei der Verschlüsselung von Nutzungs- und Inhaltsdaten zu fördern, werden im folgenden Dokument Fristen für die Verwendung der Betriebsmodi vorgegeben:

- Zeitlicher Ablauf des Umstiegs auf AES-GCM in der OSCI-Transport Bibliothek (Version vom 25.06.2018)