Koordinierungsstelle
für IT-Standards

Zeitlicher Ablauf des Umstiegs auf AES-GCM in der OSCI-Transport Bibliothek

25.06.2018

Für den Verschlüsselungsalgorithmus AES empfehlen sowohl das W3C als auch das BSI aus Sicherheitsgründen den Einsatz des Betriebsmodus GCM vorrangig vor dem CBC-Modus. Die KoSIT, als Betreiberin der OSCI-Transport Bibliothek, folgt dieser Empfehlung und hat den Betriebsmodus GCM mit der Version 1.7 für .NET und 1.7.1 für JAVA der Bibliothek im März 2017 eingeführt. Seither werden somit für den Algorithmus AES zwei Betriebsmodi parallel unterstützt: AES-CBC und AES-GCM. Das Ziel ist die Ablösung des Modus CBC durch den sichereren GCM.

Um einen geordneten Übergang von CBC zu GCM bei der Verschlüsselung von Nutzungsdaten auf Transportebene zwischen Sender und Empfänger zu fördern, wird durch die KoSIT für die OSCI-Transport Bibliothek festgelegt:

- Seit März 2017 wird AES mit GCM unterstützt.
- Bis zum 14.11.2019 wird AES mit CBC unterstützt.
- Ab dem 15.11.2019 wird ausschließlich AES mit GCM angeboten.

Um im Bereich XInneres einen geordneten Übergang bei der Verschlüsselung von Inhaltsdaten zwischen Autor und Leser sicherzustellen, wird durch die KoSIT und in Abstimmung mit der Steuerungsgruppe XInneres festgelegt, dass bei der Verschlüsselung der Inhaltsdaten im Bereich XInneres:

- bis zum 31.10.2019 AES ausschließlich mit CBC zu verwenden ist und
- ab dem 01.11.2019 AES ausschließlich mit GCM zu verwenden ist.

Wir empfehlen für den sicheren Betrieb von Fach- und Transportverfahren, die Umstellung der kryptographischen Verfahren zeitnah zu beginnen.