citeq – Scheibenstraße 109 – 48153 Münster
KRZN – Friedrich-Heinrich-Allee 130 – 47475 Kamp-Lintfort

Ansprechpartner

von DataClearing NRW

citeq
Telefon (0251) 492 – 0
Telefax (0251) 492 – 7710

Auskunft erteilt Frank Helmer
E-Mail helmer@citeq.de
Telefon (0251) 492 – 1826

KRZN
Telefon (02842) 9070 – 0
Telefax (02842) 92732 – 321

Auskunft erteilt Dr. Lars van der Grinten
E-Mail lars.van.der.grinten@krzn.de
Telefon (02842) 9070 – 321

Datum **08.07.2019**

DataClearing NRW – Newsletter 35

Sehr geehrte Damen und Herren,

der Standard OSCI-Transport sowie die XöV-Standards nutzen eine Verschlüsselung sowohl auf Transport- als auch auf Inhaltsdatenebene. Bislang wurde hier der Betriebsmodus CBC des Verschlüsselungsalgorithmus AES eingesetzt.

Im Zuge zweier Schwachstellenmeldungen in den Jahren 2017 und 2018 hat die Koordinierungsstelle für IT-Standards (KoSIT) gemeinsam mit Partnern festgestellt, dass dieser Betriebsmodus zumindest für OSCI nicht mehr sicher ist. Obwohl das Schadenspotential für OSCI als „gering“ eingestuft wird, hat die KoSIT bereits am 25.06.2018 ein Schreiben veröffentlicht, in dem der Umstieg auf den aktuellen Betriebsmodus GCM des Verschlüsselungsalgorithmus AES wie folgt festgesetzt wird:

- Die OSCI-Transport Bibliothek bietet für die Transportverschlüsselung ab dem 15.11.2019 ausschließlich AES-GCM an
- Im Standard XInneres inklusive seiner Module (XMeld, XAusländer, XPersonenstand, XPersonenstandsregister und Basismodul) ist für die Inhaltsdatenverschlüsselung ab dem 01.11.2019 ausschließlich AES-GCM zu verwenden

Die Erläuterungen und Veröffentlichungen der KoSIT finden Sie auf der KoSIT-Webseite https://www.xoev.de/downloads-2316 unter dem Punkt „OSCI 1.2“, die Handreichung vom Juni 2018 haben wir diesem Newsletter in Anlage beigefügt.

In anderen XöV-Standards gestaltet sich die Sachlage wie folgt:

- Der Betreiber des Standards XGewerbeanzeige hat im Juli 2019 mitgeteilt, dass es zum 01.05.2020 mit der Version 2.1 eine verbindliche Vorgabe zu AES-GCM geben wird.

- Der Betreiber des Standards XhD prüft derzeit die zeitlichen und fachlichen Möglichkeiten für den Umstieg auf AES-GCM.

DataClearing NRW setzt die Produkte der Fa. Governikus KG für den Intermediärsbetrieb ein. Wir weisen an dieser Stelle darauf hin, dass die an den beiden Standorten von DataClearing NRW genutzten Versionen der Software Governikus den Verschlüsselungsalgorithmus AES-GCM vollständig unterstützen und auch noch den Algorithmus AES-CBC verarbeiten können.

Die Umstellung des Verschlüsselungsalgorithmus in den einzelnen Fachverfahren wird von den jeweiligen Herstellern vorgenommen. Falls Sie zur Inbetriebnahme von AES-GCM in den Fachverfahren weitergehende Fragen haben sollten, nehmen Sie bitte Kontakt mit den Herstellern auf.

Wir wünschen Ihnen eine gute Sommerzeit und hoffentlich einige erholsame Urlaubstage!

Mit freundlichen Grüßen

Team DataClearing NRW

In eigener Sache:
Nach fast 15 Jahren intensiver Beschäftigung mit dem Thema OSCI in all seinen Facetten verlasse ich zum August 2019 die citeq und damit auch den gemeinsamen Dienst DataClearing NRW. Ich werde innerhalb der Stadt Münster eine andere Aufgabe übernehmen.
Auch wenn ich mich sehr auf diese neue Aufgabe freue, fällt es mir nicht leicht, DataClearing NRW loszulassen. Ich bedanke mich bei Ihnen für die Zusammenarbeit und für Ihr Vertrauen bei Aufbau und Betrieb dieser zu Beginn so neuen und inzwischen so vertrauten Datenübermittlung zwischen den Behörden.
Herr Dr. van der Grinten und sein Team vom KRZN werden Ihnen weiterhin als Ansprechpartner zur Verfügung stehen, mein(e) Nachfolger(in) in der citeq wird sich bei Ihnen zu gegebener Zeit vorstellen.
Ich wünsche Ihnen und Ihren Angehörigen Gesundheit und weiter viel Erfolg beim Einsatz von OSCI und XöV.

Alles Gute

Ihr Frank Helmer

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.