Die Senatorin für Finanzen
Referat 36
Neue Medien und E-Government
OSCI- Leitstelle

Freie Hansestadt Bremen

Der Senator für Finanzen · Postfach 10 15 40 · 28015 Bremen

KoopA – ADV
Verband der Clearingstellenbetriebe
Projektgruppe Meldewesen
Hersteller von Intermediärsprodukten
Nur per EMail

Auskunft erteilt Herr Steimke

Zimmer
Tel. (0421) 361 - 59 195
Fax (0421) 361 – 56 26
E-Mail frank.steimke@finanzen.bremen.de

Datum und Zeichen
Ihres Schreibens

Mein Zeichen 36-4
(bitte bei Antwort angeben)

Bremen, 15. April 2008

Umstellung auf neue Signaturalgorithmen in der OSCI Transport Infrastruktur

Sehr geehrte Damen und Herren,
das Bundesamt für die Sicherheit in der Informationstechnik hat in dem Katalog über die zur Erzeugung elektronischer Signaturen geeigneten Algorithmen dargelegt, dass der bisher genutzte Algorithmus SHA-1 für qualifizierte Signaturen nicht mehr geeignet ist. Eine Umstellung auf den Algorithmus SHA-256 bis Mitte 2008 ist geboten, zumindest für qualifizierte Signaturen.
Aus diesem Grunde muss die derzeit in Produktion befindliche OSCI-Transport Infrastruktur angepasst werden. Dies muss in abgestimmter Form erfolgen, um den Produktivbetrieb nicht zu gefährden. Dieses Schreiben dient der Information über das geplante Vorgehen. Folgende Maßnahmen wurden ergriffen bzw. sind vorgesehen:

1. Die OSCI Leitstelle hat die neue Fassung 1.3 der OSCI Transport Bibliothek bereit veröffentlicht. Diese implementiert SHA-256. Derzeit steht die neue Fassung wegen technischer Schwierigkeiten mit dem .NET Framework (Microsoft) nur in der JAVA-Implementierung zur Verfügung. Sobald diese behoben sind, wird die Bibliothek in .NET nachgeliefert.
2. Die Leitstelle hat eine Korrigenda mit Stand 10. April 2008 zu OSCI Transport herausgeben, mit der SHA-256 im Standard verankert wird. SHA-1 darf ab dem Zeitpunkt des Inkrafttretens dieser Korrigenda, in OSCI-Transport für quali-

fizierte elektronische Signaturen nicht mehr genutzt werden.
Für andere Signaturniveaus darf SHA-1 weiterhin genutzt werden. Dies halten wir angesichts der Tatsache, dass in großen Anwendungsbereichen wie z. B. dem Meldewesen qualifizierte Signaturen nicht zur Anwendung kommen, für sachgerecht. Alle Beteiligten sind aber aufgefordert, baldmöglichst SHA-1 durch SHA-256 zu ersetzen.

3. Die Korrigenda vom 10. April 2008 ist ab dem 1. Juli 2008 wirksam.
4. Hersteller von Intermediärsprodukten müssen gewährleisten, dass diese Produkte spätestens ab dem 1. Juli 2008 SHA-256 unterstützen.
5. Teilnehmer des OSCI-Transport Informationsverbundes, insbesondere also Meldebehörden bzw. Betreiber von Clearingstellen, müssen gewährleisten, dass ihre Verfahren spätestens ab dem 1. Juli 2008 eine OSCI-Transport Bibliothek einsetzen, die SHA-256 unterstützt.

Die OSCI Leitstelle wird die Marktsituation beobachten. Vorgesehen ist, zu einem angemessenen Zeitpunkt SHA-1 aus der Liste der in OSCI-Transport für die Erstellung von Signaturen zugelassenen Algorithmen vollständig zu entfernen.

Mit freundlichem Gruß

i. A. Steimke