

Welches Verschlüsselungsverfahren wird mit Smart Mail verwendet?

Grundsätzlich wird jede Mailkommunikation in und aus der Hamburg-Cloud mit TLS-Option initiiert.

Das bedeutet:

Wenn ein einliefernder Server TLS-Verschlüsselung anfordert, wird mit dieser Option geantwortet.

Ausgehende Mails werden als erstes mit TLS-Verschlüsselung angeboten. Wenn der empfangende Server die Option unterstützt, wird diese verwendet.

In allen Standard-Mail-Kommunikationen gibt es jedoch die Option auf die unverschlüsselte Kommunikation zurück zu fallen.

Um sicher zu stellen, dass E-Mails NUR über TLS-Verschlüsselung übertragen werden, müssen die betreffenden Empfänger-Domains in der Smart Mail Umgebung der Hamburg-Cloud eingetragen werden. Dieses erfolgt durch eine Anforderung an den Hamburg-Cloud Service Desk.

Danach werden die Empfänger-Domains NUR noch mit TLS-Verschlüsselung angesprochen. Es gibt kein Fallback auf unverschlüsselte Kommunikation mehr.

Wenn der Empfänger nicht entsprechend konfiguriert ist, ist keine Mail-Kommunikation mehr möglich.

Das bedeutet die Gegenseiten müssen TLS-Verschlüsselung grundsätzlich konfiguriert haben.

Zusätzlich müssen sie, um die verschlüsselte Kommunikation sicher zu stellen, diese ebenfalls für die betreffenden Domains zwingend konfigurieren.

Weitere Informationen zur TLS-Kommunikation. (Diese Information können der anfragenden Stelle zur Verfügung gestellt werden.):

Technischer AP: Hamburg-Cloud Service Desk, service@hamburg-cloud.de, +49 40 63705 808

Verwendetes Zertifikat in Smart Mail: Wildcard Zertifikat *.hamburg-cloud.de; trusted third-party CA, z.zt. Comodo CA

Managed Services: Ja, Smart Mail aus der Hamburg-Cloud

Verschlüsselung: TLS

Domain: hier die betreffende Domain angeben die zwingend mit TLS angesprochen werden soll: @firma.de

Datenspeicherung außerhalb EU: NEIN; Datenspeicherung in Hamburg, Deutschland, Rechenzentren der Hamburg-Cloud

Mail Routing: MX

Hostnamen: z.zt.: mx[01-03].hamburg-cloud.de

Seite 1 / 2

Eindeutige ID: #1210