

**Richtlinie für eine
sichere elektronische Kommunikation
mit der Stadt Greven**

Inhaltsverzeichnis

1. Ausgangslage	3
2. Verschlüsselte Kommunikation mit der Stadt Greven	3
2.1 Zentrale Verschlüsselung am E-Mail-Gateway	3
2.1.1 Austausch der Schlüssel	4
2.2 Cryptshare	4
2.3 De-Mail	4
2.4 Weitere Alternativen	5
3. Vorteile	5

Ansprechpartner:

Falls Sie uns Ihren öffentlichen Schlüssel bereitstellen möchten oder eine Frage zur verschlüsselten Kommunikation mit der Stadt Greven haben, nehmen Sie bitte Kontakt mit Ihrem Ansprechpartner im jeweiligen Fachbereich auf. Alternativ können Sie uns eine E-Mail mit Ihrem Anliegen an verschluesselung@stadt-greven.de schicken.

Versionsverzeichnis:

Version	Datum	Autor
1.0	02.09.2019	FD 1.2
1.1	19.11.2019	FD 1.2

1. Ausgangslage

Das Internet hat die Kommunikation im privaten wie im geschäftlichen Bereich stark verändert. Informationen werden im Internet beschafft. Statt zu telefonieren oder einen Brief zu schreiben, werden E-Mails versendet. Auch die Stadt Greven setzt die E-Mail oft als bevorzugtes Kommunikationsmittel ein. Die Kommunikation per E-Mail ist schnell und zuverlässig. Per E-Mail können Informationen zeitnah zur Verfügung gestellt werden, die für die weitere Bearbeitung von Prozessen erforderlich sind.

Die „normale“ E-Mail hat einen entscheidenden Nachteil: Diese E-Mail ist im Standard auf dem Übertragungsweg durch das Internet unverschlüsselt und somit ungeschützt. Unverschlüsselte E-Mails können unbemerkt eingesehen werden und trotzdem ist die E-Mail das bevorzugte Kommunikationsmittel weltweit.

Die Einführung einer Verschlüsselung bietet Vertraulichkeit und Schutz. Die verschlüsselte Kommunikation verhindert das Mitlesen durch unbefugte Dritte und gewährleistet damit Vertraulichkeit. Sie schützt Daten, ganz gleich ob es Text-, Video-, Bild- oder Sprachnachrichten sind, vor Kriminellen oder Datensammlern. Die Stadt Greven hat durch die Einführung einer zentralen Lösung direkt am E-Mail-Gateway die Möglichkeit geschaffen, E-Mails zu bestimmten Behörden und Partnern automatisch zu verschlüsseln.

Dieser Leitfaden soll dabei helfen, die möglichen Verschlüsselungsalternativen der Stadt Greven aufzuzeigen und transparent zu machen. Es soll deutlich gemacht werden, dass durch die Nutzung von Verschlüsselungstechniken zum einen ein wirtschaftlicher Nutzen erzeugt wird, zum anderen aber auch rechtliche Sicherheit gewährleistet werden kann. Denn sensible Daten wie zum Beispiel Dokumente mit personenbezogenen Informationen dürfen aus Datenschutzgründen nicht unverschlüsselt per E-Mail verschickt werden.

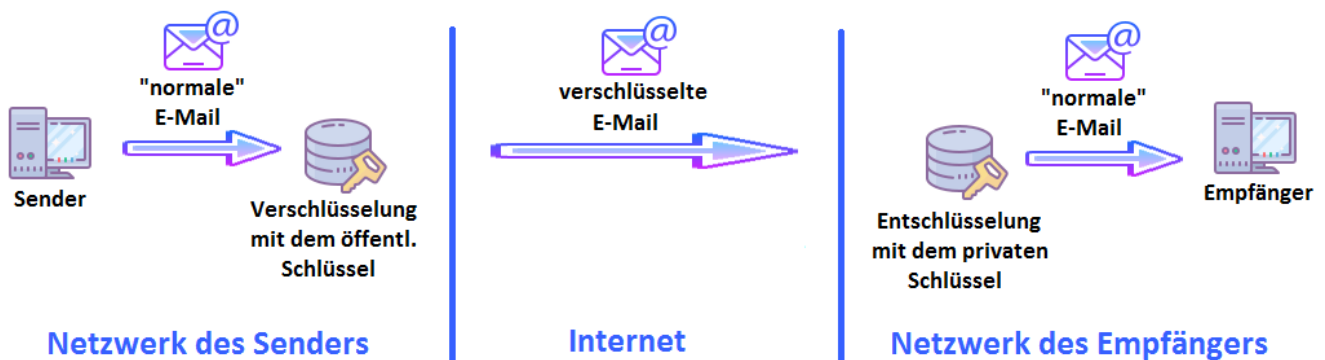
2. Verschlüsselte Kommunikation mit der Stadt Greven

Die Stadt Greven bietet zurzeit folgende Möglichkeiten der sicheren digitalen Kommunikation an:

2.1 Zentrale Verschlüsselung am E-Mail-Gateway

Die Stadt Greven hat durch die Einführung einer zentralen Lösung direkt am E-Mail-Gateway die Möglichkeit geschaffen, E-Mails zu bestimmten Behörden und Partnern automatisch zu verschlüsseln. Für die Verschlüsselung kommt S/MIME als Standard zum Einsatz.

S/MIME basiert auf einer asymmetrischen Verschlüsselung und verwendet ein Paar mathematisch verknüpfter Schlüssel - einen öffentlichen Schlüssel und einen privaten Schlüssel. E-Mails werden mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Die E-Mail kann nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden, der im alleinigen Besitz des Empfängers sein sollte. Wenn der private Schlüssel nicht kompromittiert wird, kann nur der legitime Empfänger auf die Daten zugreifen.



2.1.1 Austausch der Schlüssel

Der öffentliche Schlüssel der Stadt Greven kann auf der Internetseite https://www.greven.net/global/kontakt_neu.php heruntergeladen werden. Falls Sie ebenfalls über ein E-Mail-Gateway verfügen, welches eine E-Mail-Verschlüsselung unterstützt, können Sie oder Ihr IT-Dienstleister unseren Schlüssel direkt am Gateway einbinden. Im Anschluss können Sie alle ausgehenden E-Mails an die Stadt Greven mit diesem Schlüssel verschlüsseln.

Falls Sie kein E-Mail-Gateway besitzen, können Sie den öffentlichen Schlüssel der Stadt Greven im Zertifikatsspeicher Ihres Computer-Betriebssystems installieren. Hierzu müssen Sie einen Doppelklick auf die heruntergeladene Zertifikatsdatei machen und den Anweisungen des Assistenten folgen. Im Anschluss können Sie ausgehende E-Mails an die Stadt Greven mit einem geeigneten E-Mail-Programm verschlüsselt versenden.

Damit die Stadt Greven Ihnen ebenfalls verschlüsselte E-Mails senden kann, benötigen wir Ihren öffentlichen Schlüssel. Ein so genanntes S/MIME- oder E-Mail-Zertifikat ist bei verschiedenen Dienstleistern erhältlich. Neben kostenlosen Zertifikaten (vor allem für Privatnutzer) gibt es diverse Angebote, die sich an Business-Nutzer richten.

Wenn Sie ein Zertifikat erworben und den privaten Schlüssel in Ihr System integriert haben, teilen Sie uns bitte den Internetlink für den Download des öffentlichen Schlüssels mit oder senden Sie uns diesen per E-Mail zu. In beiden Fällen verwenden Sie bitte die E-Mail-Adresse verschluesselung@stadt-greven.de. Wir speichern Ihren öffentlichen Schlüssel in unserem E-Mail-Gateway und schicken Ihnen im Anschluss dauerhaft alle E-Mails verschlüsselt zu.

2.2 Cryptshare

Die Web-Anwendung Cryptshare ermöglicht den einfachen und sicheren Austausch vertraulicher Informationen durch die verschlüsselte Ablage von Dateien und Nachrichten auf unserem Cryptshare-Server (<https://cs.stadt-greven.de>). Der Server befindet sich im Rechenzentrum der Stadt Greven.

Bei der Ersteinrichtung erfolgt die Überprüfung des Benutzers über dessen E-Mail-Adresse. Diese Verifizierung ist für maximal 365 Tage gültig. Nach Ablauf dieser Zeit verlangt das System bei der nächsten Anmeldung eine erneute Verifizierung. Die maximale Größe für den Datenaustausch beträgt 500 MB.

Um der Stadt Greven eine verschlüsselte Nachricht zu schicken, rufen Sie in Ihrem Browser die Internetseite <https://cs.stadt-greven.de> auf und klicken auf „Bereitstellen“. Im Anschluss geben Sie ihre Absenderdaten ein und verifizieren Sie Ihre E-Mail-Adresse. Danach geben Sie einen Empfänger innerhalb der Stadt Greven an. Empfänger, die nicht auf @stadt-greven.de enden, werden vom System abgelehnt. Im nächsten Schritt können Sie eine vertrauliche Nachricht und/oder Dateianhänge hinzufügen. Anschließend können noch weitere Transferoptionen wie zum Beispiel das Ablaufdatum (max. 10 Tage) geändert oder ein zusätzliches Passwort generiert bzw. eingegeben werden. Falls Sie ein Passwort verwenden, müssen Sie dies Ihrem Ansprechpartner in der Stadt Greven, am besten telefonisch, mitteilen. Im letzten Schritt können Sie den verschlüsselten Transfer zur Stadt Greven starten.

Der Cryptshare-Server informiert Empfänger und Absender über die Vorgänge auf dem Server, d.h. Sie als Sender erhalten eine E-Mail, dass Ihre Nachricht zugestellt wurde. Wenn der Empfänger in der Stadt Greven, die Nachricht abgerufen hat, bekommen sie ebenfalls ein E-Mail. Sobald das Ablaufdatum Ihrer Nachricht erreicht wurde, erhalten Sie eine E-Mail, dass die Daten gelöscht wurden und ob der Empfänger die Daten heruntergeladen hat oder nicht. Danach ist der Vorgang abgeschlossen.

2.3 De-Mail

De-Mail ermöglicht eine nachweisbare und vertrauliche elektronische Kommunikation. De-Mail ist leicht anzuwenden und bietet Sicherheitsmerkmale, die E-Mails fehlen. Dadurch wird die elektronische Kommunikation von Bürgerinnen und Bürgern, Unternehmen und Behörden deutlich besser geschützt. Betrieben wird De-Mail von staatlich zugelassenen Anbietern.¹

¹ <https://www.cio.bund.de> am 06.05.2019

De-Mail verhindert die ungewollte Öffentlichkeit von privaten Daten durch Verschlüsselung der Transportwege, durch eindeutige Identifizierung der Teilnehmenden sowie durch den nachweisbaren Versand und Empfang der Nachrichten. Auch die staatliche Akkreditierung der De-Mail-Anbieter dient der Kontrolle der De-Mail-Systeme und dem Schutz Ihrer Daten vor Zugriffen durch Unbefugte. Der Datenschutz spielt also eine zentrale Rolle bei der Akkreditierung von De-Mail-Anbietern und bei der täglichen Nutzung von De-Mail.¹

Die Stadt Greven erreichen Sie unter folgender DE-Mail-Adresse: info@stadt-greven.de-mail.de

Bei Fragen zur DE-Mail empfehlen wir Ihnen die Internetseiten vom Beauftragten der Bundesregierung für Informationstechnik¹ oder die Internetseiten des Bundesamtes für Informationssicherheit (BSI)².

2.4 Weitere Alternativen

Es gibt eine Menge von Möglichkeiten die Kommunikation zwischen E-Mail-Sender und E-Mail-Empfänger zu verschlüsseln. Die E-Mail-Server der Stadt Greven unterstützen zum Beispiel die TLS-Verschlüsselung. Allerdings sind unsere Systeme nicht so konfiguriert, dass eine TLS Zwangsverschlüsselung (forced TLS) vorliegen muss. Außerdem möchten wir Sie bitten, vom Versand verschlüsselter E-Mail-Anhänge abzusehen. Diese werden von unserem E-Mail-Gateway blockiert. Bitte haben Sie Verständnis, dass die Stadt Greven nicht jede Alternative unterstützen kann.

3. Vorteile

Eine verschlüsselte E-Mail-Kommunikation erfüllt die Anforderungen an die EU-DSGVO und behält die wirtschaftlichen Vorteile einer digitalen Kommunikation:

- Kosten für Papier, Briefumschlag und Porto entfallen
- Personalaufwand für Kuvertierung der Briefe und Transport zum Zusteller entfallen
- Transportzeit der Zusteller entfallen
- Digitale Weiterverarbeitung auf Seiten der Empfänger wird unterstützt

Unverschlüsselte E-Mails bergen ein großes Sicherheitsrisiko. Sie sind während des Versands jederzeit unbemerkt einsehbar – vergleichbar mit einer Postkarte. Mit einer Verschlüsselung bleibt die Vertraulichkeit Ihrer Kommunikation gewahrt. Eine verschlüsselte Kommunikation unterstützt die Forderung des Datenschutzes, sensible personenbezogene oder geschäftskritische Informationen nur mittels eines sicheren Übertragungsweges auszutauschen.

² <https://www.bsi.bund.de>