# Verschlüsselte E-Mail-Kommunikation mit der Stadt Hagen (Leitfaden)

STADT HAGEN

HABIT

| | |
|---|---|
| Version: | 1.4 |
| Stand: | 18.12.2017 |
| Zuständigkeitsbereich: | HABIT/41, HABIT/1 |

# 1. Inhaltsverzeichnis

1. Inhaltsverzeichnis ..... 2
2. Vorbereitung ..... 3
2.1. Hintergrund ..... 3
2.2. Sicheres Passwort ..... 4
2.3. E-Mail-Programm installieren und konfigurieren für den E-Mail-Empfang und -Versand ..... 4
3. Verschlüsselte E-Mails empfangen ..... 4
3.1. Zertifikat beantragen ..... 5
3.2. Installation des eigenen Zertifikats/ Schlüsselpaars ..... 5
3.3. Versand des eigenen öffentlichen Schlüssels an Stadt Hagen ..... 5
4. Verschlüsselte E-Mails an die Stadt Hagen versenden ..... 6
4.1. Download des öffentlichen Schlüssels der Stadt Hagen ..... 6
4.2. Installation des öffentlichen Schlüssels der Stadt-Hagen ..... 6
4.3. Installation des Root-Zertifikats ..... 6
4.4. Test der Verschlüsselung ..... 7
5. Kontakt ..... 8
6. Hinweise auf Software: ..... 8

# 2. Vorbereitung

## *2.1. Hintergrund*

Einen normalen Brief werden Sie immer in einen Umschlag stecken, so dass nur der von Ihnen ausgesuchte Adressat diesen lesen kann und niemand sonst unterwegs. Selbst wenn Sie Ihren Postboten sympathisch finden, werden Sie ihm den Inhalt des Briefs nicht zur Kenntnis geben. Belanglose Dinge wie Grüße samt Temperaturangabe vom Urlaubsort senden Sie auf einer Postkarte, weil Ihnen egal ist, wer in den Poststellen am Urlaubsort, an Flughäfen und am Heimatort mitliest.

E-Mails sind elektronische Postkarten. Wenn Sie sich zur Mittagspause verabreden, ist die E-Mail ein schnelles und unkompliziertes Mittel und jeder auf dem Weg dieser Mail zum Empfänger kann mitlesen, was Sie von dem betreffenden Restaurant halten. Na und?!

Personensensible Daten, z.B. die Ihrer Kunden, Mandanten, Patienten sind nicht belanglos! Sie gehören weder auf eine Postkarte noch in eine E-Mail!. Den Beschäftigten der Stadt Hagen ist es verboten, derartige Daten zu senden, sei es auch nur in der Antwort auf Ihre Mail. Die im Folgenden vorgestellte Art der Verschlüsselung gilt in der Fachwelt als sicher vor auch gut ausgerüsteten Hackern.

Ihre E-Mail an die Stadt Hagen müssen Sie verschlüsseln, wenn sie personensensible Daten enthält. Sie können von der Stadt Hagen auch nur verschlüsselte E-Mails mit personensensitiven Daten erhalten!

Sie benötigen dazu

- ein Mailprogramm wie z.B. Thunderbird©, MS Outlook Express© oder MS Outlook©,
- ein Zertifikat oder auch “Schlüsselpaar” für sich selbst sowie den öffentlichen Schlüssel der Stadt Hagen, in Ihrem Mailprogramm hinterlegt.

Ersteres ist in der Regel bekannt, bequem und teilweise kostenlos aus dem Internet herunterladbar.
Ein „Zertifikat“ für die Verschlüsselung von E-Mails ist begrifflich meist unbekannt: Für die Verschlüsselung liefert Ihnen das Zertifikat[1] 2 so genannte Schlüssel (eigentlich sind es nur Zahlenfolgen):

- Den privaten Schlüssel halten Sie geheim. Er kann nicht installiert werden ohne das Passwort, dass nur Ihnen bekannt sein sollte. Mit dem privaten Schlüssel entschlüsselt das Mailprogramm automatisch an Sie gerichtete E-Mails, insofern sie an Ihr E-Mail-Postfach gerichtet sind.

[1] Das Zertifikat hat seinen Namen bekommen, weil es auf einem höheren Niveau auch Ihre Identität bestätigen kann; Sie könnten E-Mails sogar rechtswirksam elektronisch signieren mit der gleichen Gültigkeit wie eine handschriftliche Signatur unter einem Papierdokument. Aber diese Funktion wird nicht für die E-Mail-Verschlüsselung benötigt.

- Den öffentlichen Schlüssel geben Sie Ihren Kommunikationspartnern, z.B. der Stadt Hagen (s.u.). Mit ihm können diese die E-Mails an Sie verschlüsseln. Der Clou: Nur der Besitzer Ihres geheimen privaten Schlüssels (Sie!) kann diese Mails entschlüsseln, der öffentliche Schlüssel reicht hierfür nicht und lässt auch nicht auf den privaten schließen. Das heißt auch: Wollen Sie an die Stadt Hagen E-Mails senden, benötigen Sie den öffentlichen Schlüssel der Stadt Hagen. Wie das alles (für eine wirklich lange Nutzungszeit) einzurichten ist, lesen Sie unten.

Für die E-Mail-Verschlüsselung wird nur ein „Class1“[2]-Zertifikat benötigt, dies ist meist kostengünstig oder kostenlos auch für gewerbliche Nutzer zu erwerben.

### *2.2. Sicheres Passwort*

Im Laufe des Verfahrens wird es erforderlich werden, ein sicheres Passwort zum Zugriffsschutz der Zertifikatsdatei auf der Festplatte einzugeben. Bitte überlegen Sie sich ein sicheres Passwort, das nicht aus echten Wörtern besteht, mindestens 8 Zeichen unterschiedlicher Zeichenklassen enthält (Großbuchstaben, Kleinbuchstaben, Satzzeichen, Ziffern). Am einfachsten und sichersten sind Anfangsbuchstaben + Ziffern + Satzzeichen erdachter Sätze oder Sprichwörter, z.B. „Wh7W,an2K.“ für „Wir haben 7 Wellensittiche, aber nur 2 Katzen.“ o.ä.

### *2.3. E-Mail-Programm installieren und konfigurieren für den E-Mail-Empfang und -Versand*

Hier ist das E-Mail-Programm Ihrer Wahl gemeint. Die Signierung und Verschlüsselung von Mails samt Anhang kann nur über ein Mailprogramm wie z.B. Thunderbird©, MS Outlook Express© oder MS Outlook© vorgenommen werden. (Um Mails auf dem sogenannten Webbrowser, also direkt auf der Website von Freenet©, GMX©, AOL©, etc. verschlüsseln zu können, müssten Sie Ihrem Webprovider Ihren höchst vertraulichen privaten Schlüssel überlassen! Es ist prinzipiell aber abzuraten, seinen privaten Schlüssel Dritten zugänglich zu machen!)

Derartige Programme können gekauft werden, im Fall von Thunderbird© ist auch eine kostenlose Nutzung möglich. Für die Einrichtung sind zahlreiche Beschreibungen im Internet hinterlegt, so dass hier nichts wiederholt werden muss.

## 3. Verschlüsselte E-Mails empfangen

Hierzu müssen Sie ein Zertifikat/ Schlüsselpaar erwerben, Ihren privaten Schlüssel installieren und Ihren öffentlichen Schlüssel bereitstellen. Im Einzelnen:

[2] Class1 bedeutet, dass lediglich die E-Mail-Adresse verifiziert wurde, ansonsten gibt es keine Garantie für die Authentizität des Absenders. Für die reine E-Mail-Verschlüsselung ist dieser Umstand aber nicht interessant bzw. das Class1-Zertifikat schon nutzbar.

### 3.1. Zertifikat beantragen

Für die E-Mail-Verschlüsselung wird lediglich ein „Klasse 1“- bzw. „Class 1“-Zertifikat von einem Zertifikatsanbieter, einem sogenannten Trustcenter benötigt.

Selbst erstellte Zertifikate sind nicht verwendbar. Achten Sie darauf, dass es kein PGP-/ GnuPG-/OpenPG-Zertifikat ist, sondern vom Typ „S/MIME“ bzw. „X.509“ !

Falls Sie mehrere E-Mail-Adressen haben, beachten Sie bitte, dass das erworbene Zertifikat nur für eine E-Mail-Adresse gilt, die Sie bei Antragstellung angegeben haben. Nur E-Mails an diese Adresse können Sie entschlüsseln.

Im Internet finden sich zahlreiche Angebote[3]. Wie Sie das Zertifikat erwerben bzw. erhalten können, ist vom jeweiligen Trust Center abhängig und i.d.R. dort gut beschrieben.

### 3.2. Installation des eigenen Zertifikats/ Schlüsselpaars

Installieren Sie das Zertifikat in Ihrem E-Mail-Programm.

Möglicherweise wurde es im Laufe der Zertifikatsbeantragung in Ihrem Browser-Programm automatisch installiert (oftmals bei „Internet Explorer“ der Fall), dann können Sie es dort exportieren als Datei und diese dann im E-Mail-Programm importieren. Export beim Internet Explorer (hier Version 8.0): Menüpunkte „Extras, Internetoptionen“, dann Reiter „Inhalte“, (mittig) Button „Zertifikate“, Reiter „eigene Zertifikate“, Button „Exportieren …“. Dann weiter dem Assistenten folgen.

### 3.3. Versand des eigenen öffentlichen Schlüssels an Stadt Hagen

Senden Sie an stadtverwaltung@stadt-hagen.de eine signierte Mail. Die Signierung (= Versand mit Ihrem öffentlichen Schlüssel als Anhangsdatei) können Sie im Fenster des E-Mail-Programms der neu erstellten Mail anweisen.

Natürlich können Sie den öffentlichen Schlüssel auch an jeden anderen Kommunikationspartner versenden, von dem Sie künftig E-Mails verschlüsselt erhalten möchten.

[3] Die Stadt Hagen darf keine Werbung für bestimme Trustcenter machen, daher hier nur der allgemeine Hinweis: Googeln Sie z.B. mit Begriffen wie „class1 zertifikat kostenlos“, wenn Sie lediglich die hier behandelte E-Mail-Verschlüsselung betreiben wollen und achten Sie darauf, dass erforderlichenfalls die gewerbliche Nutzung erlaubt ist. Für rechtsverbindliche Mails mit einem Class3-Zertifikat werden nur Trustcenter, also Zertifikatsanbieter akzeptiert, die von der Bundesnetzagentur zugelassen wurden. Für eine vollständige Liste möglicher Anbieter suchen Sie also auf der Homepage der Bundesnetzagentur (http://www.bundesnetzagentur.de) einfach nach „Qualifizierte elektronische Signatur“, dann weiter nach „Veröffentlichungen“ und „Zertifikatsdiensteanbieter“.

# 4. Verschlüsselte E-Mails an die Stadt Hagen versenden

## *4.1. Download des öffentlichen Schlüssels der Stadt Hagen*

Den Schlüssel finden Sie im Impressum von www.hagen.de. Mit „Ziel speichern unter…“ oder ähnlicher Bezeichnung bei Klick mit rechter Maustaste auf den Link können Sie ihn herunterladen.

## *4.2. Installation des öffentlichen Schlüssels der Stadt-Hagen*

- Bei Nutzung von Thunderbird©: Die Schlüsseldatei als Server-Zertifikat installieren, unter den Menüpunkten „Extras, Einstellungen“, Reiter „Erweitert“ und „Zertifikate“, dann mit Button „Zertifikate“ im Reiter „Server“ mit Button „Importieren…“die unter 5.1. heruntergeladene Datei importieren.

- Bei Nutzung von MS Outlook© müssen Sie die Datei im Zertifikatsspeicher der MS Office©-Produkte installieren, das funktioniert über den Internet Explorer© (hier Version 8.0): Menüpunkte „Extras, Internetoptionen“, dann Reiter „Inhalte“, (mittig) Button „Zertifikate“ Dort Reiter „Andere Personen“ und Button „Importieren…“ die unter 5.1. heruntergeladene Datei auswählen.

- Das neue Zertifikat markieren. Mit Button „Vertrauen bearbeiten“ (Thunderbird©) oder „Erweitert …“ (Internet Explorer©) den Schlüssel der Stadt Hagen als „vertrauenswürdig“ (Thunderbird©)/ „Sichere E-Mail“ (Outlook©) kennzeichnen.

## *4.3. Installation des Root-Zertifikats*

Zertifikate von Firmen und Privatleuten sind abgeleitet vom Root- oder „Wurzel“-Zertifikat des Herausgebers, im Falle des Zertifikats der Stadt Hagen ist dies die Fa. procilon IT-Solutions GmbH. Deren Root-Zertifikate muss ebenfalls im eMail-Programm vorhanden sein, damit die Verschlüsselung funktioniert.

- Laden Sie sich das „procilon GROUP Customer RootCA 01“ sowie das „procilon GROUP Customer CA – SMIME“-Zertifikat von der Homepage „procilon IT-Solutions GmbH“ (LINK) herunter. Hilfsweise wird auch im Impressum der Stadt Hagen dieses Root-Zertifikat zum Download angeboten.

- Die Schlüsseldatei unter „Zertifizierungsstellen“ (Begriff z.B. im Thunderbird©-Dialog; im Internet Explorer©: „Vertrauenswürdige Stammzertifizierungsstellen“ oder „Zwischenzertifizierungsstellen“) installieren.

- Das neue Zertifikat markieren. Mit Button „Vertrauen bearbeiten“ (Thunderbird©) oder „Erweitert …“ (Internet Explorer©) den Schlüssel der Stadt Hagen als „vertrauenswürdig“ (Thunderbird©)/ „Sichere E-Mail“ (MS Outlook©) kennzeichnen.

## *4.4. Test der Verschlüsselung*

Senden Sie bitte Ihre erste verschlüsselte Mail an die Stadt Hagen:

- Verwenden Sie als E-Mail-Adresse stadtverwaltung@stadt-hagen.de und
- im Betreff Ihren Gesprächspartner bei der Stadt.
- Weisen Sie die Verschlüsselung dieser Mail an und schließlich …
- bitte senden.

Besten Dank!

# 5. Kontakt

Bei Fragen verwenden Sie bitte den HABIT-Direktkontakt
http://www.hagen.de/irj/portal/Kontakt?rid=DKA-HABIT

oder

wenden Sie sich an

Stadt Hagen
Hagener Betrieb für Informationstechnologie (HABIT)
Postfach 4249
58042 Hagen

E-Mail: HABIT@stadt-hagen.de

# 6. Hinweise in eigener Sache

Die im Text genannte Software ist nur beispielhaft und nur wegen ihrer allgemeinen Verbreitung genannt. In keiner Weise werden damit Empfehlungen ausgesprochen. Eine eigene Meinungsbildung über die jeweilige Marktlage entsprechender Softwareprodukte ist unbedingt empfohlen. Die genannten Konfigurationsbeispiele waren unserer Ansicht nach allerdings notwendig, da von nahezu allen Herstellern die Installation von Verschlüsselungsmöglichkeiten nur unzureichend unterstützt wird: Die vielfach üblichen Installationsassistenten fehlen in diesem Sektor leider völlig. Für eine sichere und sachgerechte Verwendung der Verschlüsselung ist eigenes Wissen über die Zusammenhänge aber ohnehin erforderlich. Wir hoffen, mit dem vorliegenden Leitfaden eine Unterstützung in dieser Richtung gegeben zu haben.

Hagen, im Dezember 2017