Information
Technology
Solutions

User-Guide

der
Information Technology Solutions (IT Solutions) der TU Wien
als Auftragnehmer & Serviceerbringer
kurz: Serviceerbringer

für die
Institute/Organisationseinheiten/Mitarbeiter der TU Wien

als Auftraggeber & Servicenehmer
kurz: Servicenehmer

zum Service
‚Sicheres E-Mail'[i]

Digitale Signatur
und
Verschlüsselung für E-Mails
via
TU Wien Secure E-Mail Gateway

als

Funktionale Erweiterung zu upTUdate

Stand: 6. Februar 2020
Version 1.8

1 Allgemeine Informationen....3
2 Wie können ‚schützenswerte Daten' via E-Mail transportiert werden?....3
3 Was ist das "TU Secure E-Mail Gateway"?....4
4 Was ist eine Digitale Signatur?....4
5 Was ist eine Digitale Verschlüsselung?....6
6 Wie arbeitet das "TU Secure E-Mail Gateway"?....7
6.1 Funktionen:....8
7 Self-Service Aktivierung TU Wien Secure E-Mail Gateway....8
7.1 Verschlüsselung mit dem TU Wien Secure E-Mail Gateway....10
7.2 Was bewirkt ein #ENC beim upTUdate-externen Empfänger?....10
7.3 Notifikationen bei Secure E-Mail Gateway Nutzung....11
7.4 BeispielNotifikation....12
8 Umstieg von lokalen Client- S/MIME Zertifikaten auf TU Wien Secure E-Mail Gateway....13
8.1 Deaktivierung der lokalen S/MIME Zertifikate im E-Mail Client....13
9 TU Wien Secure E-Mail Webmail-Service....17

1 Allgemeine Informationen

Jedem Mitarbeiter, jeder Mitarbeiterin der TU Wien (Servicenehmer_in) stellt TU.it (Serviceerbringer_in) ab Dienstbeginn automatisch eine auf Servern der TU Wien gehostete Mail- und Kalenderlösung zur Verfügung (Service upTUdate).

Spätestens seit Mai 2018 DSGVO sind ‚schützenswerte' Daten im E-Mail-Verkehr besonders zu behandeln.

Das Versenden an eine *@tuwien.ac.at – E-Mail-Adresse garantiert NICHT, dass der E-Mail-Kommunikations-Verkehr innerhalb TU Wien verbleibt (z.B. können Weiterleitungen nicht ausgeschlossen werden).

2 Wie können ‚schützenswerte Daten' via E-Mail transportiert werden?

Variante 1: von TU.it zentral gemanagtes TU Wien Secure E-Mail Gateway für upTUdate-Benutzer

Variante 2: selbstverantwortlich mit lokalen S/MIME Zertifikaten im E-Mail Client

Damit Sie an der sicheren E-Mail-Kommunikation teilnehmen können, benötigen Sie – sowie Ihr_e Kommunikationspartner_in - ein persönliches S/MIME Zertifikat, welches ein Schlüsselpaar (privater Schlüsselteil für Sie sowie öffentlicher Schlüsselteil für Ihre_n Kommunikationspartner_in) enthält.

Als upTUdate-Benutzer_in stellen wir Ihnen eine Lösung via TU Wien Secure E-Mail Gateway zur Verfügung.

Wenn Sie die TU Wien Secure E-Mail Gateway-Lösung verwenden, wird dieses Schlüsselpaar (S/MIME Zertifikat) für Sie vom TU Wien Sicheren E-Mail Gateway erstellt und verwaltet.

Für alle Studierenden und Mitarbeiter_innen stellen wir auch die Möglichkeit lokaler S/MIME Zertifikate zur Signierung und Verschlüsselung auf Endgeräten zur Verfügung.

Sie müssen das notwendige Schlüsselpaar selbst beziehen, und dieses auf all ihren Geräten (Desktop, Laptop, Mobile, Tablet, etc) selbst verwalten und selbst regelmäßig erneuern.

3 Was ist das “TU Secure E-Mail Gateway”?

Das TU Wien Secure E-Mail Gateway wird in den Datenverkehr zwischen Mailservern geschaltet und kümmert sich um folgende Funktionalitäten:

- Digitale Signatur (Erstellung und Verifikation)
- Verschlüsselung und Entschlüsselung des Nachrichteninhalts
- Schlüssel und S/MIME Zertifikatsmanagement

4 Was ist eine Digitale Signatur?

Die digitale Signatur ist eine informationstechnologische Möglichkeit die Identität einer E-Mail-Adresse zu bestätigen.

Digitale Signaturen sind notwendig, um in einer digitalisierten Kommunikation die Unversehrtheit einer Nachricht oder eines Dokuments zu garantieren und den Ursprung zu einer bestimmten Person oder einem bestimmen Ausgangspunkt rückführbar zu gestalten.

Die Voraussetzung der digitalen Signatur ist das oben erwähnte S/MIME Zertifikat, welches aus öffentlichem und privatem Schlüssel besteht.

Der private Teil Ihres Schlüsselpaares wird für die Signatur Ihrer E-Mail verwendet. Der öffentliche Teil wird mit der E-Mail mitgeschickt, damit der Empfänger Ihre Signatur verifizieren kann.

Eine E-Mail mit digitaler Signatur ist nicht verschlüsselt.

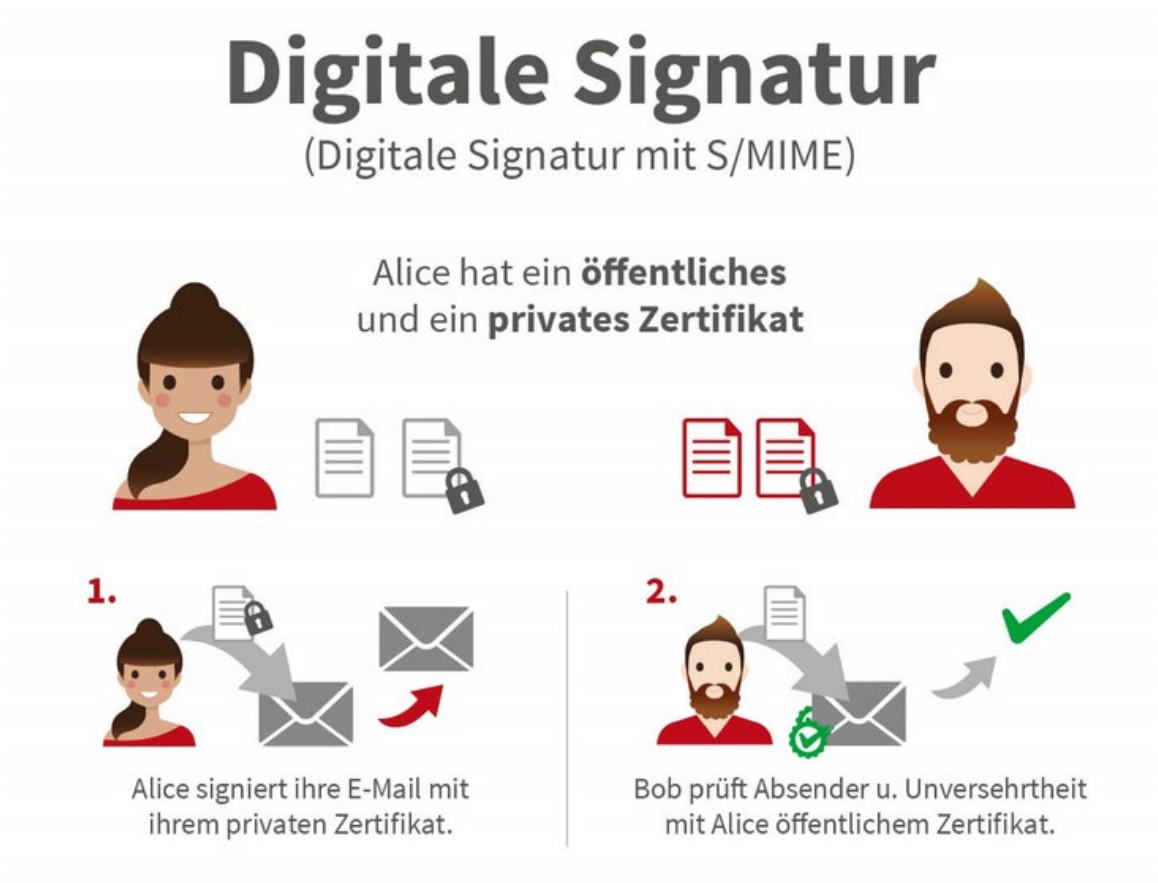


Abbildung 1: Digitale Signatur (cc-by-sa: www.reddoxx.com)

Erklärung zur Abbildung: Ein Zertifikat besteht aus einem Schlüsselpaar, welches wiederum aus einem öffentlichen und privaten Schlüsselteil besteht.

In der Regel ist davon auszugehen, dass seitens der Empfänger keine Probleme bei der Verifikation Ihrer digital signierten Nachrichten entstehen. Fast jeder Mail-Client im beruflich genutzten Umfeld kann eine digital signierte Nachricht interpretieren und auf die Unversehrtheit prüfen, wie auch die Absenderzertifikate verifizieren.

Mit der Nutzung der Digitalen Signatur ist für Ihren Empfänger Ihre Identität sichergestellt jedoch keine Interaktion notwendig. Antwortet Ihr Empfänger ohne Interaktion = ohne Zertifikat, haben Sie keinen Identitätsnachweis.

5 Was ist eine Digitale Verschlüsselung?

Um E-Mails zu verschlüsseln wird der öffentliche Schlüsselteil der jeweiligen Kommunikationspartner genutzt.

Um verschlüsselte E-Mails lesen zu können, wird der private Schlüsselteil der jeweiligen Kommunikationspartner genutzt.

Das TU Wien Secure E-Mail Gateway sammelt die zur Verschlüsselung geeigneten öffentlichen Schlüssel der externen Kommunikationspartner (=externe Mailadressen) und kann bei Bedarf automatisch die Ver- bzw. Entschlüsselung durchführen.

Abbildung 2: S/MIME (cc-by-sa: www.reddoxx.com)

Erklärung zur Abbildung: Ein Zertifikat besteht aus einem Schlüsselpaar, welches wiederum aus einem öffentlichen und privaten Schlüsselteil besteht.

Der Transport aller E-Mails innerhalb des upTUdate Services läuft auf verschlüsselten Transportwegen ab. Daher ist innerhalb des upTUdate Services keine zusätzliche Inhaltsverschlüsselung notwendig.

6 Wie arbeitet das "TU Secure E-Mail Gateway"?

Als funktionale Erweiterung zum upTUdate Service bieten wir Ihnen das TU Wien Secure E-Mail Gateway an, um „sichere E-Mails" [i] mittels Digitaler Signatur bzw. Verschlüsselungsfunktion nutzen zu können.

Mithilfe des TU Wien Secure E-Mail Gateways werden die S/MIME Zertifikate vom TU Wien Secure E-Mail Gateway - im Gegensatz zu den selbständig lokal auf jedem Arbeitsplatz zu verwalteten Zertifikaten - für Sie verwaltet.

Details zur Servicebeschreibung sind auch auf unserer Homepage unter Services → Kooperation und Kommunikation → E-Mail und Kalender upTUdate (E-Mail u. Kalender f. Mitarb.) → Sicheres E-Mail (https://www.it.tuwien.ac.at/services/kooperation-und-kommunikation/e-mail-und-kalender/uptudate-e-mail-u-kalender-f-mitarb/sicheres-e-mail/) zu finden.

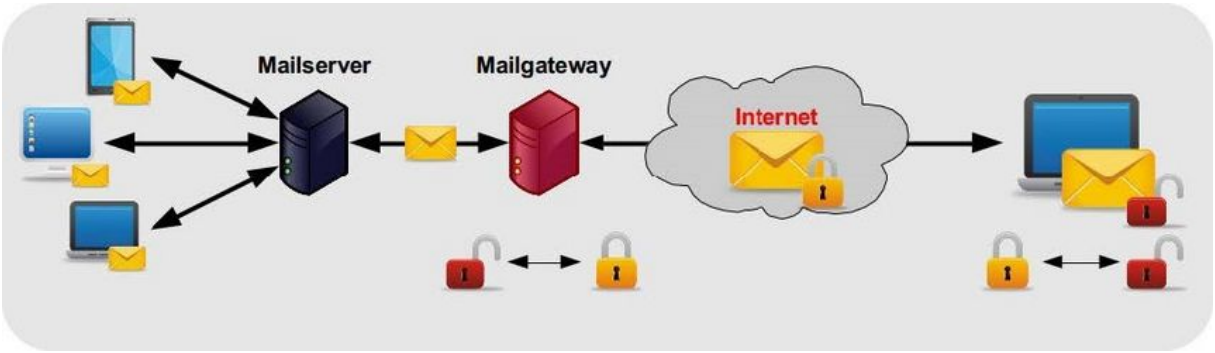


Abbildung 3: Funktionsweise E-Mail Gateway

6.1 FUNKTIONEN:

- Das TU Wien Secure E-Mail Gateways unterstützt upTUdate Kunden_innen, welche das TU Wien Secure E-Mail Gateway-Service aktiviert haben, durch Anbringung der digitalen Signatur an alle E-Mails, welche das upTUdate Service verlassen. Innerhalb upTUdate wird der E-Mail-Verkehr nicht signiert.
- Das TU Wien Secure E-Mail Gateway unterstützt Sie, Ihre E-Mails, welche das upTUdate Service verlassen, verschlüsselt zu übermitteln (siehe Kommando #enc Punkt 7.1).
- UpTUdate-externe Kommunikationspartner, von denen das TU Secure E-Mail Gateway noch keinen öffentlichen Schlüssel gespeichert hat, bekommen eine E-Mail-Information (siehe Punkt 7.2f Notifikationen) mit dem Verweis auf unser TU Wien Secure E-Mail Webmail-Service.
- Sobald der externe Kommunikationspartner ebenfalls digital signiert an Sie sendet oder ein S/MIME Zertifikat beim TU Wien Secure E-Mail Webmail-Service hinterlegt, wird dadurch der öffentliche Schlüsselteil des Kommunikationspartner automatisch im TU Wien Secure E-Mail Gateway gespeichert. Ab diesem Zeitpunkt können zu verschlüsselnde E-Mails an diesen Kommunikationspartner vom TU Wien Secure E-Mail Gateway verschlüsselt versandt werden, da der Kommunikationspartner dadurch nachgewiesen hat, dass er über seinen eigenen privaten Schlüsselteil verfügt und daher die E-Mail entschlüsseln kann.

7 Self-Service Aktivierung TU Wien Secure E-Mail Gateway

Melden Sie sich bitte beim TU.it Online Account Management unter https://oase.it.tuwien.ac.at/ZID-DB.amsAccounts an. Dort finden Sie Ihren upTUdate Account und können dort das TU Wien Secure E-Mail Gateway aktivieren:

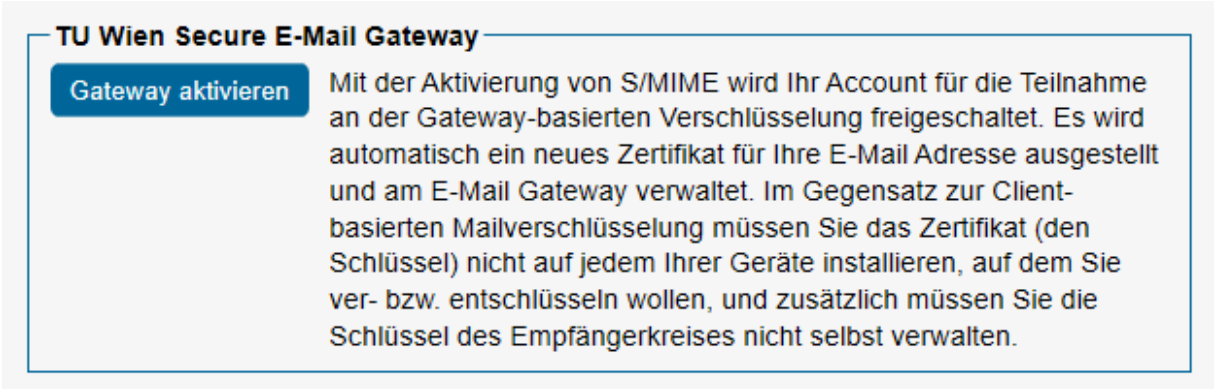


Abbildung 4: E-Mail Gateway Aktivierung

Die Aktivierung bedeutet, dass Sie das TU Wien Secure E-Mail Gateways nutzen. Das hierfür neu generierte S/MIME Zertifikat wird vom TU Wien Secure E-Mail Gateway verwaltet.

Ab diesem Zeitpunkt werden folgende Funktionen aktiv:

- ALLE Ihre E-Mails an Empfänger außerhalb upTUdate werden immer mit einer Digitalen Signatur versehen.
- Sie können den Verschlüsselungsmechanismus für E-Mail außerhalb upTUdates mit unten beschriebenen Kommandos (Punkt 7.1 #enc ...) auslösen

Die Kommunikation innerhalb upTUdate muss nicht zusätzlich inhaltsverschlüsselt werden, da sie bereits transportverschlüsselt ist.

Eine Deaktivierung ist nicht direkt für Sie wählbar, weil dadurch ein größerer Administrationsaufwand mit der Zertifikatsverwaltung verbunden ist. Bitte kontaktieren sie uns dazu via der Mailadresse: help@it.tuwien.ac.at

Der **Import** von bestehenden *lokalen S/MIME Zertifikaten auf das* TU Wien Secure E-Mail Gateway ist **NICHT** möglich. Durch die Aktivierung wird für Sie ein *neues S/MIME Zertifikat* erzeugt und dieses am TU Wien Secure E-Mail Gateway hinterlegt.

Eine parallele Verwendung beider S/MIME Zertifikate ist möglich, aber NICHT empfohlen.

⇒ Hinweis: Bewahren Sie das bisherige lokale S/MIME Zertifikat inklusive Passwort auf jeden Fall weiterhin auf, weil Sie dieses für bereits empfangenen, verschlüsselte E-Mails unbedingt benötigen.

Ihre Kommunikationspartner_innen verwenden das bisherige (lokale) S/MIME Zertifikat solange dieses gültig ist. Ihr neues S/MIME Zertifikat ist in Verwendung, sobald ein Versenden und Empfangen einer signierten E-Mail erfolgreich stattgefunden hat.

Solange dem TU Wien Secure E-Mail Gateway kein öffentlicher Schlüssel Ihres Kommunikationspartners bekannt ist, wird Ihrem Kommunikationspartner eine E-Mail-Information (siehe Punkt 7.3 & 7.4) über das Vorliegen einer verschlüsselten E-Mail mit Verweis auf das TU Wien Secure E-Mail Gateway zugesandt.

⇒ Hinweis: Bitte bedenken Sie, dass Ihr lokales S/MIME Zertifikat ein Ablaufdatum hat und E-Mail-Clients sehr unterschiedlich ab diesem Zeitpunkt reagieren können. Es besteht die Gefahr, dass Sie dann verschlüsselte E-Mails nicht mehr öffnen können.

⇒ Hinweis: Bitte nutzen Sie die Betreffzeile NIE für vertrauliche Informationen!
Der Standard für Verschlüsselung sieht nur eine Verschlüsselung für den „Body" der E-Mail-Nachricht vor. Dies bedeutet, die Betreffzeile wird niemals verschlüsselt und ist somit von allen an der Kommunikation beteiligten Systemen les- und auswertbar.

7.1 VERSCHLÜSSELUNG MIT DEM TU WIEN SECURE E-MAIL GATEWAY

Wenn Sie eines der folgenden Kommandos in der Betreffzeile an den Anfang stellen, wird Ihre E-Mail an upTUdate-externe Empfänger_Innen verschlüsselt übermittelt.

- **#encrypt oder #enc**

Die Zeichenfolgen „#encrypt" oder ‚#enc' werden vom TU Wien Secure E-Mail Gateway in weiterer Folge entfernt und sind für einen externen Empfänger nicht sichtbar.

Da innerhalb des upTUdate Services nicht verschlüsselt wird und diese E-Mails daher nicht vom TU Wien Secure E-Mail Gateway bearbeitet werden, bleiben diese Zeichenfolgen im Betreff erhalten. So erkennt der Empfänger den besonders schützenswerten Inhalt.

7.2 WAS BEWIRKT EIN #ENC BEIM UPTUDATE-EXTERNEN EMPFÄNGER?

- **Erste mit #enc verschlüsselte E-Mail an upTUdate-externen Empfänger:**

  Dem TU Wien Secure E-Mail **Gateway ist noch kein öffentlicher Schlüssel Ihres Kommunikationspartners bekannt, aus diesem Grund wird Ihrem Kommunikationspartner eine E-Mail-Information (siehe Punkt 7.3 & 7.4) über das Vorliegen einer verschlüsselten E-Mail mit Verweis auf das TU Wien Secure E-Mail Gateway zugesandt.**

- Der Empfänger erhält mit dieser E-Mail-Information = Notifikation ‚Registrierung zum Erhalt sicherer Nachrichten' (siehe Punkt 7.4) folgende Möglichkeiten:

  - eine mit S/MIME oder PGP signierte Antwort-E-Mail (durch ‚Klick auf den entsprechenden Button') zu retournieren

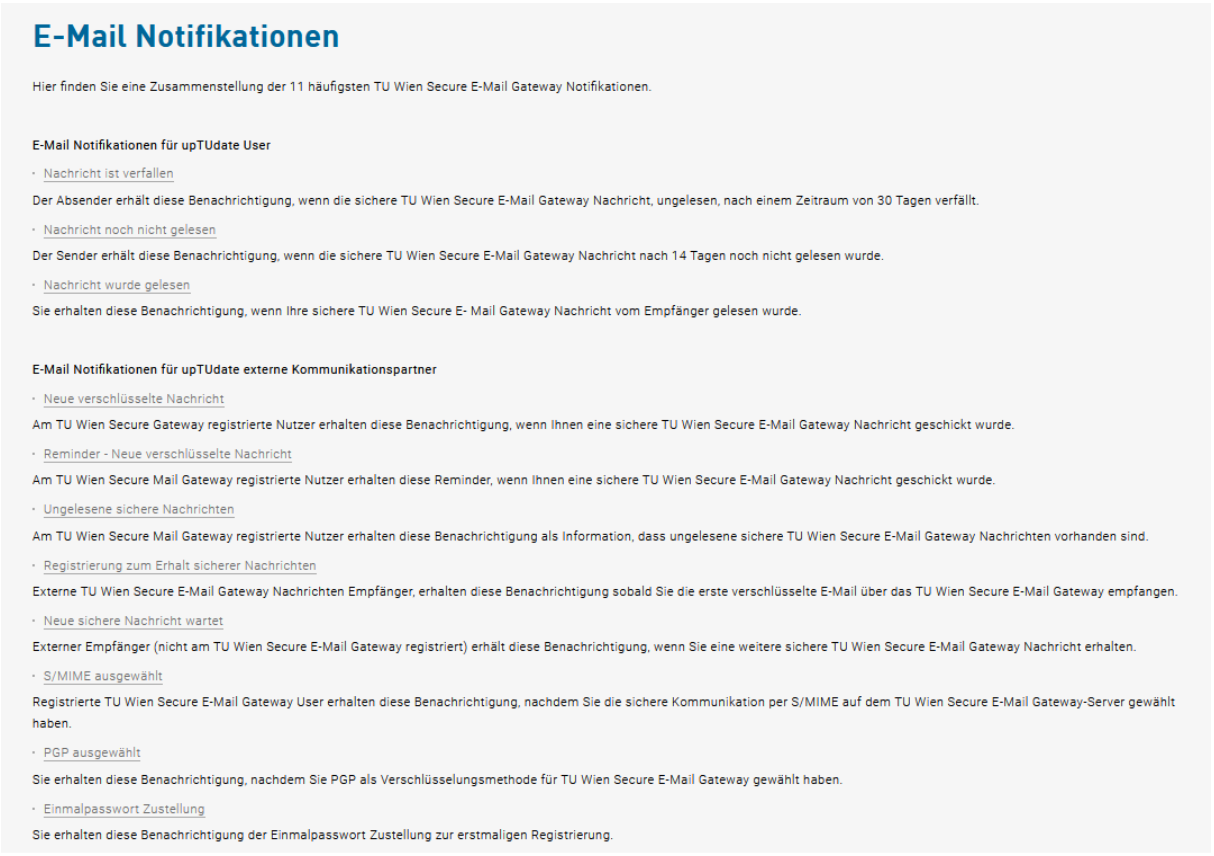
  - eine Webmail-Portal-Registrierung (durch ‚Klick auf den entsprechenden Button') auszuführen

- Sobald der externe Kommunikationspartner ebenfalls digital signiert an Sie sendet oder ein S/MIME Zertifikat beim TU Wien Secure E-Mail Webmail-Service hinterlegt, wird der **öffentliche Schlüsselteil des Kommunikationspartner automatisch** im TU Wien Secure E-Mail **Gateway gespeichert**.

  Ab diesem Zeitpunkt können zu verschlüsselnde E-Mails an diesen Kommunikationspartner vom TU Wien Secure E-Mail Gateway **OHNE NOTIFIKATION** verschlüsselt versandt werden. Der Kommunikationspartner hat dadurch nachgewiesen, dass er über seinen eigenen privaten Schlüsselteil verfügt und die E-Mail entschlüsseln kann.

7.3 NOTIFIKATIONEN BEI SECURE E-MAIL GATEWAY NUTZUNG

Notifikationen sind anlassbezogene Benachrichtigungen an den E-Mail-Versender oder an den E-Mail Empfänger, die vom Gateway verschickt werden.



E-Mail Notifikationen

Hier finden Sie eine Zusammenstellung der 11 häufigsten TU Wien Secure E-Mail Gateway Notifikationen.

E-Mail Notifikationen für upTUdate User

- Nachricht ist verfallen

Der Absender erhält diese Benachrichtigung, wenn die sichere TU Wien Secure E-Mail Gateway Nachricht, ungelesen, nach einem Zeitraum von 30 Tagen verfällt.

- Nachricht noch nicht gelesen

Der Sender erhält diese Benachrichtigung, wenn die sichere TU Wien Secure E-Mail Gateway Nachricht nach 14 Tagen noch nicht gelesen wurde.

- Nachricht wurde gelesen

Sie erhalten diese Benachrichtigung, wenn Ihre sichere TU Wien Secure E- Mail Gateway Nachricht vom Empfänger gelesen wurde.

E-Mail Notifikationen für upTUdate externe Kommunikationspartner

- Neue verschlüsselte Nachricht

Am TU Wien Secure Gateway registrierte Nutzer erhalten diese Benachrichtigung, wenn Ihnen eine sichere TU Wien Secure E-Mail Gateway Nachricht geschickt wurde.

- Reminder - Neue verschlüsselte Nachricht

Am TU Wien Secure Mail Gateway registrierte Nutzer erhalten diese Reminder, wenn Ihnen eine sichere TU Wien Secure E-Mail Gateway Nachricht geschickt wurde.

- Ungelesene sichere Nachrichten

Am TU Wien Secure Mail Gateway registrierte Nutzer erhalten diese Benachrichtigung als Information, dass ungelesene sichere TU Wien Secure E-Mail Gateway Nachrichten vorhanden sind.

- Registrierung zum Erhalt sicherer Nachrichten

Externe TU Wien Secure E-Mail Gateway Nachrichten Empfänger, erhalten diese Benachrichtigung sobald Sie die erste verschlüsselte E-Mail über das TU Wien Secure E-Mail Gateway empfangen.

- Neue sichere Nachricht wartet

Externer Empfänger (nicht am TU Wien Secure E-Mail Gateway registriert) erhält diese Benachrichtigung, wenn Sie eine weitere sichere TU Wien Secure E-Mail Gateway Nachricht erhalten.

- S/MIME ausgewählt

Registrierte TU Wien Secure E-Mail Gateway User erhalten diese Benachrichtigung, nachdem Sie die sichere Kommunikation per S/MIME auf dem TU Wien Secure E-Mail Gateway-Server gewählt haben.

- PGP ausgewählt

Sie erhalten diese Benachrichtigung, nachdem Sie PGP als Verschlüsselungsmethode für TU Wien Secure E-Mail Gateway gewählt haben.

- Einmalpasswort Zustellung

Sie erhalten diese Benachrichtigung der Einmalpasswort Zustellung zur erstmaligen Registrierung.

Abbildung 5. E-Mail Notifikationen bei Gateway Nutzung

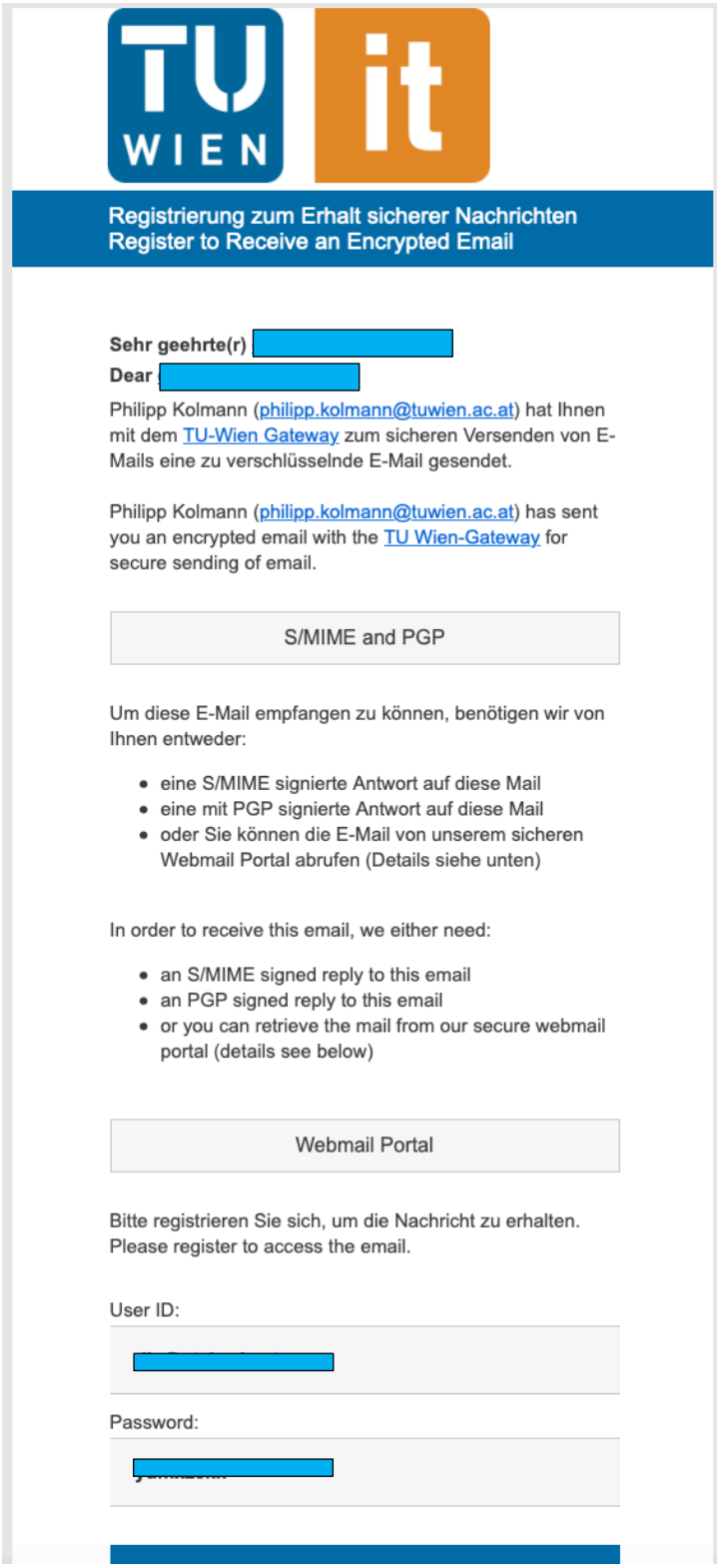
Eine Zusammenstellung der 11 am häufigsten vorkommenden Notifikationen findet sich unter folgendem Link, wobei Erweiterungen ständig eingepflegt werden:

https://www.it.tuwien.ac.at/services/kooperation-und-kommunikation/e-mail-und-kalender/uptudate-e-mail-u-kalender-f-mitarb/sicheres-e-mail-gateway/e-mail-notifikationen /

7.4 BEISPIELNOTIFIKATION

Registrierung zum Erhalt sicherer Nachrichten

Externe Empfänger erhalten diese Notifikation, sobald die erste zu verschlüsselnde E-Mail über das TU Wien Secure E-Mail Gateway gesendet wird:



Registrierung zum Erhalt sicherer Nachrichten
Register to Receive an Encrypted Email

Sehr geehrte(r) [redacted]
Dear [redacted]

Philipp Kolmann (philipp.kolmann@tuwien.ac.at) hat Ihnen mit dem TU-Wien Gateway zum sicheren Versenden von E-Mails eine zu verschlüsselnde E-Mail gesendet.

Philipp Kolmann (philipp.kolmann@tuwien.ac.at) has sent you an encrypted email with the TU Wien-Gateway for secure sending of email.

S/MIME and PGP

Um diese E-Mail empfangen zu können, benötigen wir von Ihnen entweder:

- eine S/MIME signierte Antwort auf diese Mail
- eine mit PGP signierte Antwort auf diese Mail
- oder Sie können die E-Mail von unserem sicheren Webmail Portal abrufen (Details siehe unten)

In order to receive this email, we either need:

- an S/MIME signed reply to this email
- an PGP signed reply to this email
- or you can retrieve the mail from our secure webmail portal (details see below)

Webmail Portal

Bitte registrieren Sie sich, um die Nachricht zu erhalten.
Please register to access the email.

User ID:

Password:

Geschwärzte Information

Abbildung 6: Beispielnotifikation

8 Umstieg von lokalen Client- S/MIME Zertifikaten auf TU Wien Secure E-Mail Gateway

Der Umstieg von lokalen S/MIME Zertifikaten auf die TU Wien Secure E-Mail Gateway basierte Verschlüsselung erfolgt in folgenden Schritten:

8.1 DEAKTIVIERUNG DER LOKALEN S/MIME ZERTIFIKATE IM E-MAIL CLIENT

Outlook:

1. Zum Deaktivieren der lokalen S/MIME Zertifikate in Outlook öffnen Sie bitte den Reiter Datei und gehen auf Optionen

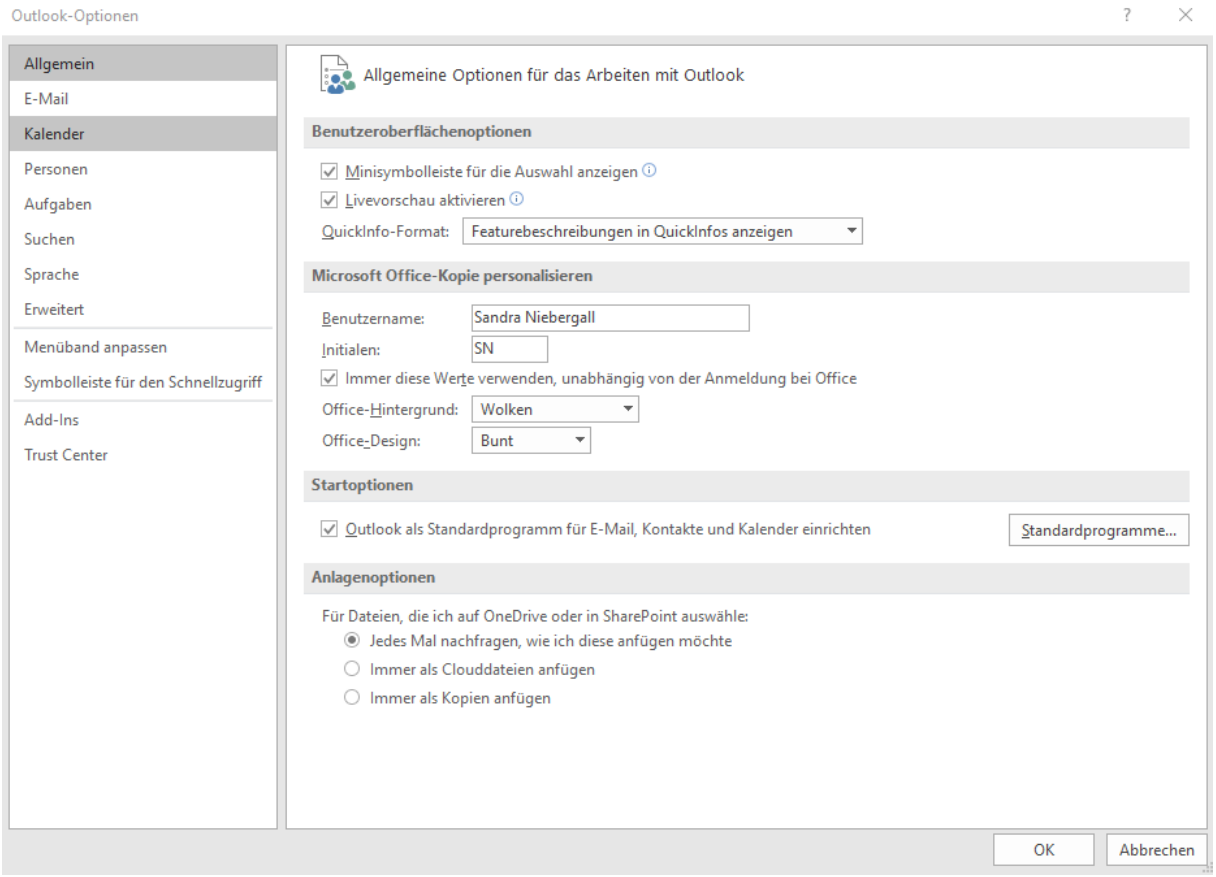


Abbildung 7: Outlook: Datei –> Optionen

2. Wechseln Sie nun zum Menüpunkt „Trust Center“ und betätigen Sie den Button „Einstellungen für das Trust Center“

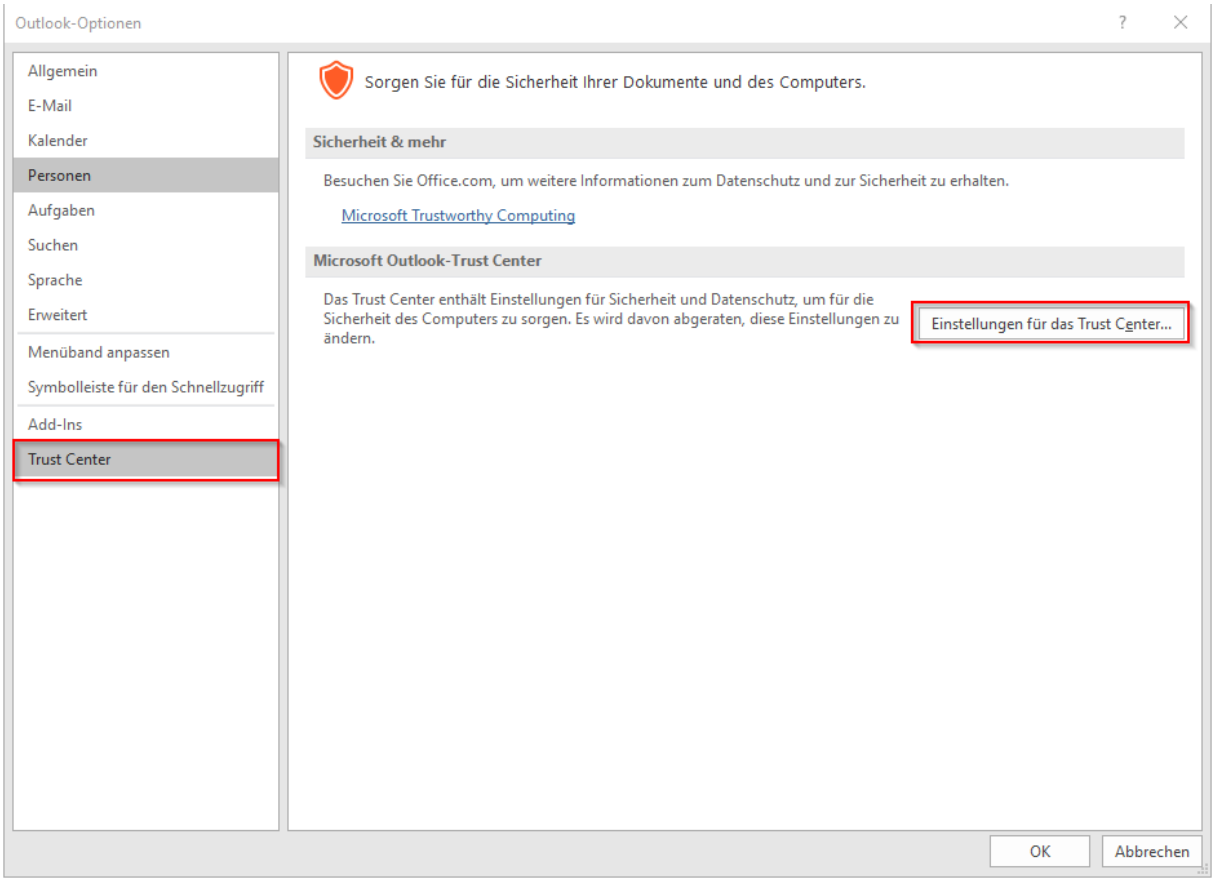


Abbildung 8: Outlook: Trust Center –> Einstellungen für das Trust Center

3. Wählen Sie hier den Menüpunkt „E-Mail-Sicherheit“

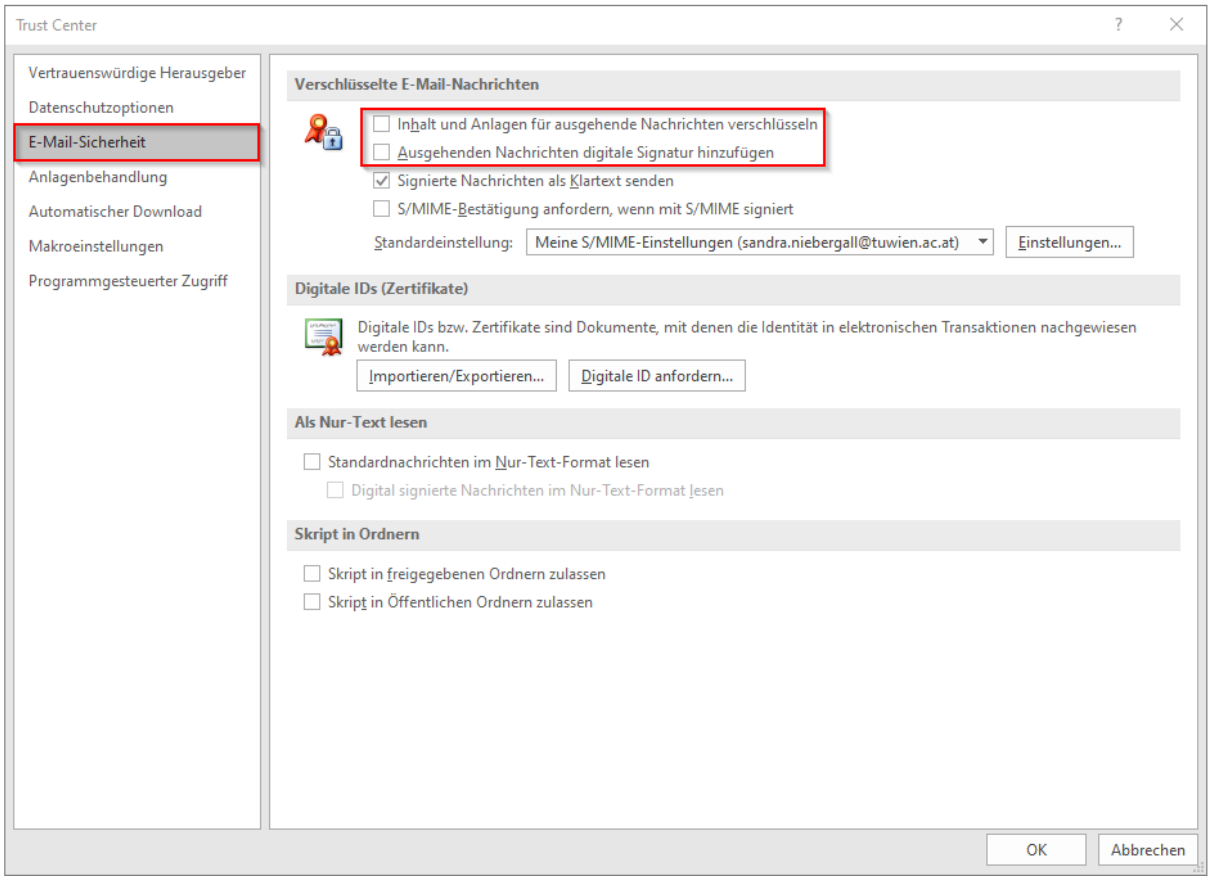


Abbildung 9: Outlook: E-Mail-Sicherheit

4. Entfernen Sie die ersten beiden Haken unter dem Abschnitt „Verschlüsselte E-Mail-Nachrichten
5. Bestätigen Sie mit OK

Thunderbird-Client:

1. Öffnen Sie in Thunderbird „Konten-Einstellungen“ und wählen Sie im entsprechenden E-Mail-Konto den Punkt „S/MIME-Sicherheit“

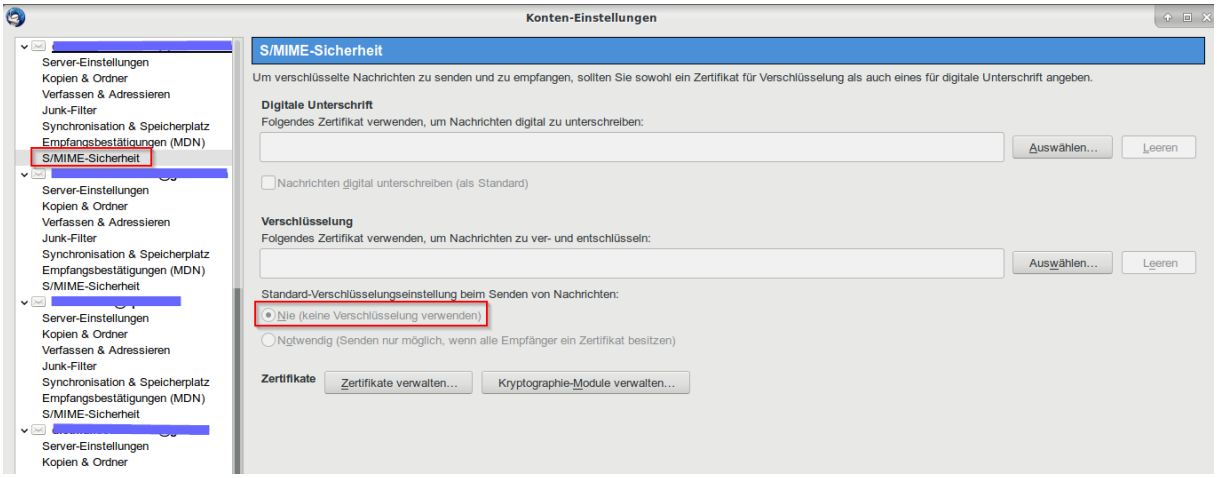


Abbildung 10: Thunderbird: S/MIME Sicherheit

2. Unter der Option Verschlüsselung setzen Sie ein Haken auf „nie“

3. Bestätigen Sie mit OK

9 TU Wien Secure E-Mail Webmail-Service

Wenn der_die Empfänger_in einer verschlüsselten E-Mail (weder ein S/MIME Zertifikat noch PGP Zertifikat (eine andere Verschlüsselungsmethode)) besitzt, dann kann die E-Mail nur noch über das TU Wien Secure E-Mail Gateway Webmail über eine verschlüsselte HTTPS Verbindung abgerufen werden.

Im Rahmen des Webmail-Services können die Empfänger_Innen nach Registrierung am TU Wien Secure E-Mail Webmail Gateway mit dem Initial-Passwort aus der Registrierungs-E-Mail (siehe Punkt 7.4) ein selbst gewähltes Passwort zur sicheren Verwendung wählen und dieses Service solange nutzen, bis sie selbst in der Lage sind mit S/MIME oder PGP Zertifikat unmittelbarer (d.h. ohne Webmail-Service) an der Kommunikation teilzunehmen.

Die aktuelle Umsetzung betrifft exklusiv die Nuzter_innen von upTUdate:

- Schützenswerte Inhalte können automatisch gesichert werden
- Die individuelle Kommunikationspartner müssen sich nicht um die Administration der Schlüssel und Zertifikate selbst kümmern

Ein Webmail-Service wird für die Kommunikationspartner angeboten, die keine persönlichen S/MIME oder PGP Zertifikate haben.

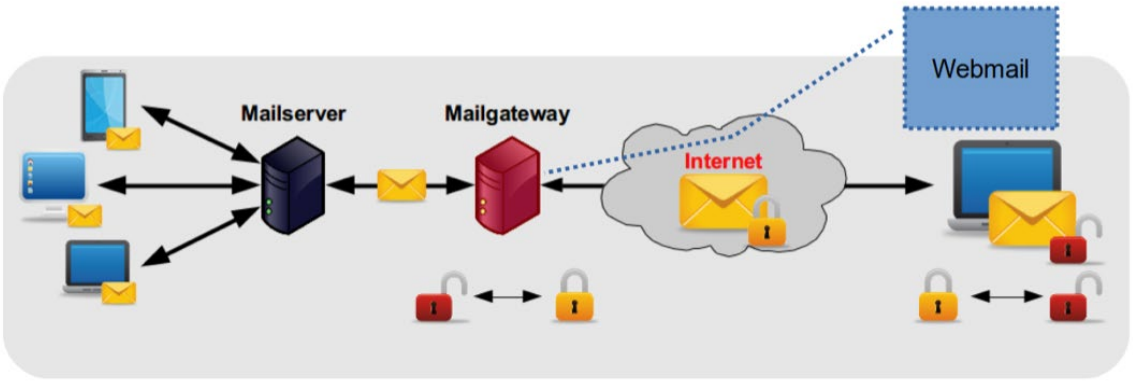


Abbildung 11: Webmail

Abbildung 1: Digitale Signatur (cc-by-sa: www.reddoxx.com)....5
Abbildung 2: S/MIME (cc-by-sa: www.reddoxx.com)....6
Abbildung 3: Funktionsweise E-Mail Gateway....7
Abbildung 4: E-Mail Gateway Aktivierung....8
Abbildung 5. E-Mail Notifikationen bei Gateway Nutzung....11
Abbildung 6: Beispielnotifikation....12
Abbildung 7: Outlook: Datei –> Optionen....13
Abbildung 8: Outlook: Trust Center –> Einstellungen für das Trust Center....14
Abbildung 9: Outlook: E-Mail-Sicherheit....15
Abbildung 10: Thunderbird: S/MIME Sicherheit....16
Abbildung 11: Webmail....17

Tabelle: Dokumentwartung

Version	Datum	Durchgeführte Änderungen
1.8	6.2.2020	Überarbeitung
1.7	30.1.2020	Überarbeitung
1.6	29.1.2020	Überarbeitung
1.5	15.1.2020	Überarbeitung
1.4	10.1.2020	Überarbeitung
1.3	9.01.2020	Überarbeitung
1.2	20.12.2019	Erstes Kundenfeedback
1.1	19.12.2019	Beispiel-Notifikation eingefügt
1.0	15.12.2019	Entwurf, Erstversion, Anpassungen
0.9	13.12.2019	Erstversion (Vorschlag durch rund²)

Endnoten:

[i] das Wording Sicheres E-Mail wird seit Mai 2018 als Begrifflichkeit für diesen Strang der Digitalisierungsstrategie der TU Wien genutzt