E-Mail-Verschlüsselung

03.07.2024 11:16:47

FAQ-Artikel-Ausdruck

Kategorie:	Kommunikation & Kollaboration::E-Mail	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	14:08:54 - 28.06.2024

Schlüsselwörter

E-Mail Verschlüsselung Einstieg LDAP PKI

Lösung (öffentlich)

Die TU Dresden nutzt die Public-Key-Infrastruktur des DFN-Vereins ([1]DFN-PKI) zur Ausstellung, Verteilung und Überprüfung von Zertifikaten. Dabei kommt S/MIME (Secure/Multipurpose Internet Mail Extensions) als standardisiertes Verfahren für die Verschlüsselung und das Signieren von E-Mails zum Einsatz.

Ohne digitale Signatur kann jede E-Mail sehr einfach manipuliert und die Absendeseite der E-Mail nicht überprüft werden. Die digitale Signatur einer E-Mail hat folgende Vorteile: Die Empfangsseite der E-Mail kann überprüfen, ob die Nachricht nur von der angegebenen Person stammt. Die Empfangsseite der E-Mail kann überprüfen, ob die Nachricht auf dem Weg nicht manipuliert wurde. (Integrität)

Voraussetzungen
- Zum Versand einer verschlüsselten E-Mail benötigen Sie ein persönliches Zertifikat:
[2]Anleitung zur Beantragung eines persönlichen Zertifikats

- Das Zertifikat muss im lokalen E-Mail-Client bzw. Betriebssystem eingebunden werden:
[3]Anleitungen für die Einbindung des persönlichen Zertifikats

- Außerdem muss das Zertifikat der Empfangsseite bekannt sein.
(siehe Abschnitt „Zertifikat der Empfangsseite erhalten“)

Persönliches Zertifikat

Notieren und merken Sie sich das bei der Beantragung vergebene Passwort für Ihr persönliches Zertifikat und sichern Sie die Zertifikatsdatei auf Ihrem Gerät. Der Download der Zertifikatsdatei ist ausschließlich bei der Beantragung möglich. Ohne die Zertifikatsdatei oder das Passwort ist es nicht möglich, das Zertifikat zu nutzen. In diesem Fall muss ein neues beantragt werden.

Laufzeit

Zertifikate besitzen eine begrenzte Laufzeit von 2 Jahren, in der sie gültig sind. Läuft ein Zertifikat aus, erhalten Sie rechtzeitig eine Information per E-Mail. Sie müssen dann ein neues Zertifikat beantragen.

Abgelaufene Zertifikate

Abgelaufene Zertifikate und die dazugehörigen Passwörter sollten weiterhin gespeichert und im E-Mail-Client eingebunden bleiben. Nur so ist es möglich, damit verschlüsselte (ältere) E-Mails weiterhin zu entschlüsseln.

Veröffentlichung

Alle persönlichen Zertifikate und Zertifikate von Funktionsadressen werden automatisch im globalen Adressbuch von Exchange und LDAP-Verzeichnis der DFN-PKI (siehe unten) bereitgestellt, damit der Austausch verschlüsselter E-Mails möglich ist.
Die TU Dresden ist rechtlich verpflichtet, die Angaben (E-Mail-Adresse, Zertifikat) zur Verschlüsselung der Beschäftigten in einem öffentlich zugänglichen Verzeichnis bereitzustellen. Die rechtliche Verpflichtung ergibt sich aus § 2 Abs. 1 Satz 3 des Sächsischen E-Government-Gesetz (SächsEGovG): „Für die elektronische Kommunikation sind Verschlüsselungsverfahren anzubieten und grundsätzlich anzuwenden.“

Zertifikat der Empfangsseite erhalten

Über das Exchange-Protokoll eingebundene E-Mail-Clients wie bspw. Gnome Evolution oder Microsoft Outlook können ohne weitere Einrichtung auf das globale Adressbuch zugreifen. Darüber lassen sich alle Angehörigen der TU Dresden finden und der E-Mail-Client ruft deren Zertifikate automatisch ab.
Falls Ihr Mail-Client nicht über Exchange verbunden ist bzw. Sie TUD-externe Personen kontaktieren möchten, können Sie eine der folgenden Varianten zum Erhalt des Zertifikats verwenden.

Variante 1: Austausch einer signierten E-Mail

Zum Versand einer verschlüsselten E-Mail muss das Zertifikat der Empfangsseite bekannt sein. Dazu müssen die Schlüssel initial über eine mit dem Zertifikat signierte E-Mail ausgetauscht werden.

Beispiel: Person A schickt eine mit ihrem persönlichen Zertifikat signierte E-Mail an Person B. Person B kennt nun das Zertifikat von Person A und kann ihr direkt eine verschlüsselte E-Mail schicken.

Variante 2: Verzeichnisdienst einbinden DFN PKI LDAP

Die DFN PKI bietet ein öffentliches LDAP (Lightweight Directory Access Protocol) Verzeichnis an, das als DFN-weites Adressbuch mit E-Mail Adressen und persönlichen Zertifikaten genutzt werden kann. Sie können das LDAP-Verzeichnis als Adressbuch in Ihrem E-Mail Programm einbinden und dadurch einfach und komfortabel Personen und deren Zertifikate finden und ihnen verschlüsselte E-Mails schicken. Das Verzeichnis enthält nahezu alle Zertifikate aus der alten DFN-PKI und zusätzlich die von SECTIGO ausgestellten Zertifikate der TU Dresden und einiger anderer Organisationen (Stand April 2024 sind das einige Max-Planck-Institute). Es ist möglich, dass die Zertifikate weiterer Organisationen hinzukommen.

Mittels eines LDAP-Browsers können Sie das DFN PKI Verzeichnis auch direkt durchsuchen:

Hostname: ldap.pca.dfn.de
Port: 389 (auch mit SSL) bzw. bei LDAPS 636
Basis-DN: o=DFN-Verein, c=DE

Einrichtung im E-Mail-Klient Je nach eingesetztem E-Mail-Klient ist ein Zugriff auf die Kontakte oder Zertifikate möglich, bedarf aber möglicherweise eine Einbindung des Verzeichnisdienstes in das Programm:

E-Mail-Klient

Kontakte

Zertifikate

automatischer Zugriff ohne Einrichtung

Apple Mail für macOS ✓ - -
[4]Anleitung

GNOME Evolution für Linux ✓ ✓ ✓
(nur für TUD-externe Kontakte notwendig)

Microsoft Outlook für macOS ✓ ✓ ✓
([5]nur für TUD-externe Kontakte notwendig)

Microsoft Outlook für Windows ✓ ✓ ✓
([6]nur für TUD-externe Kontakte notwendig)

Mozilla Thunderbird ✓ ✓ -
[7]Anleitung

[1] https://www.pki.dfn.de/ueberblick-dfn-pki
[2] https://faq.tickets.tu-dresden.de/v/ItemID=1026
[3] https://faq.tickets.tu-dresden.de/s/Keyword=E-Mail,Einrichtung,Zertifikat
[4] https://faq.tickets.tu-dresden.de/v/ItemID=488
[5] https://faq.tickets.tu-dresden.de/v/ItemID=490
[6] https://faq.tickets.tu-dresden.de/v/ItemID=511
[7] https://faq.tickets.tu-dresden.de/v/ItemID=513