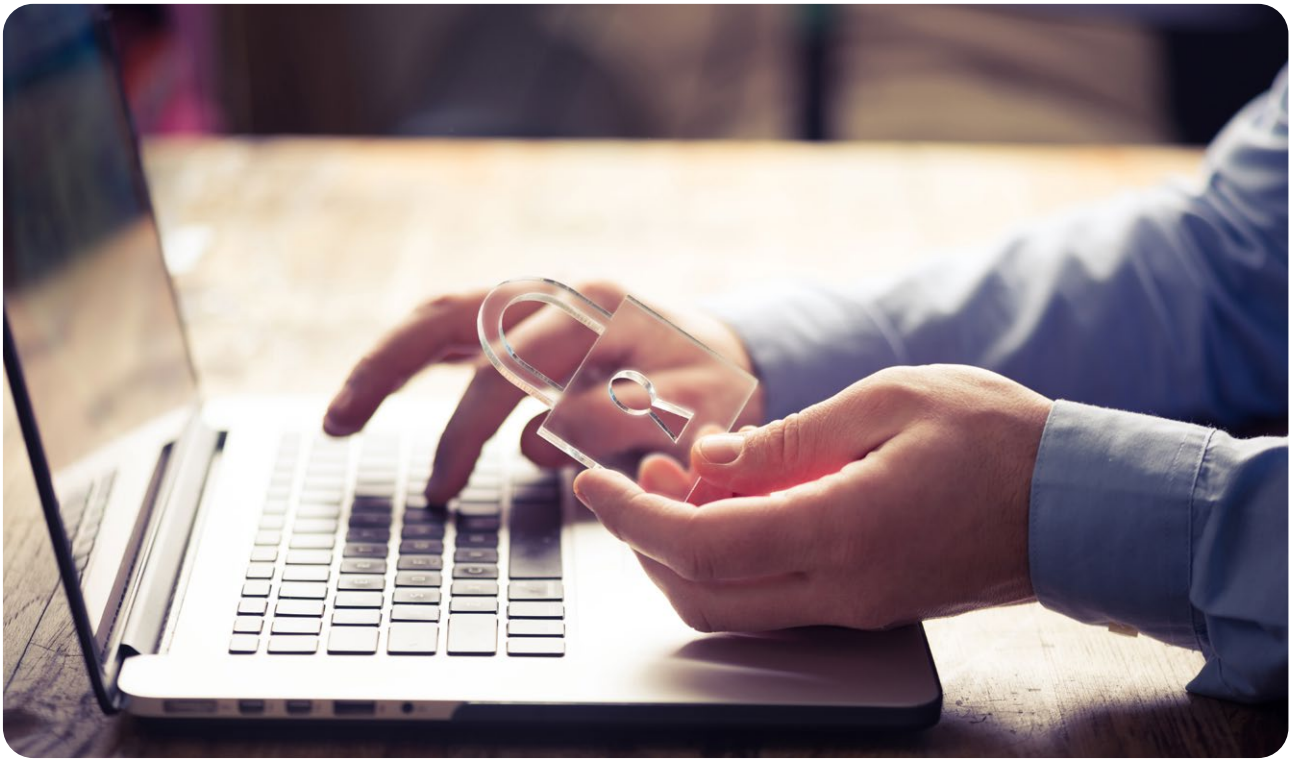
LEISTUNGSBESCHREIBUNG

Sichere E-Mail-Verschlüsselung

Für Behörden und Kommunen



Datenschutz in Behörden und Kommunen

Die europäische Datenschutzgrundverordnung (EU-DSGVO), die am 25. Mai 2018 in Kraft getreten ist, gibt Bürgern mehr Mitspracherecht, was mit ihren Daten in Behörden oder Kommunen passiert. Diese Grundverordnung umfasst beispielsweise das Recht zur Überprüfung und Recht auf Vergessen von Daten.

Darüber hinaus beinhaltet die DSGVO aber auch erweiterte Informations- und Reaktionspflichten. Wenn es zu Datenlecks, beispielsweise in Form von Hackerangriffen, kommt, müssen davon betroffene Organisationen die Bürger schnell und umfassend informieren.

Damit eine derartige Situation gar nicht erst eintritt, ist der Schutz der E-Mail-Kommunikation essentiell. Zudem ist er auch gesetzlich gefordert, wenn es um die Übertragung personenbezogener Daten geht.

Absicherung Ihrer E-Mail-Kommunikation

Einfallstor E-Mail
Eine der größten Schwachstellen in der IT-Infrastruktur, und damit Einfallstor für Datendiebstahl sowie Spionage, sind E-Mails. Daher ist die Absicherung von E-Mail-Daten und -Informationen durch Verschlüsselung und Signatur so wichtig; denn Firewalls, Virenscanner oder Spamschutz-Maßnahmen decken diesen Bereich der E-Mail-Sicherheit nicht ab.

Die Lösung für Behörden und Kommunen
Im behördlichen Umfeld hat sich der Standard S/MIME für die Verschlüsselung und Signatur von E-Mails fest etabliert. Diese Lösung basiert auf einem asymmetrischen Verschlüsselungsverfahren mit zwei Schlüsseln. Die technische Umsetzung erfolgt über clientbasierte oder serverbasierte Verschlüsselungslösungen. Letztere verschlüsseln und entschlüsseln alle E-Mails zentral auf einem sogenannten Secure E-Mail Gateway.

Bei der clientbasierten Verschlüsselung übernehmen hingegen die Rechner des Absenders und Empfängers selbst die Verschlüsselungsaufgaben. In der technischen Praxis werden beide Lösungen oft kombiniert: Gateways für Standard-E-Mails, Clients für besonders sicherheitskritische E-Mails und Anhänge.

Digitale Zertifikate
Der Einsatz digitaler Zertifikate stellt sicher, dass die Nachricht tatsächlich vom angegebenen Absender stammt. Bei der zertifikatsbasierten Verschlüsselung wird das Schlüsselpaar mit einem digitalen Zertifikat verbunden, das die Identitätsinformationen des Besitzers beinhaltet (zum Beispiel Name und E-Mail-Adresse).

Digitale Zertifikate sind auch die Voraussetzung dafür, E-Mails elektronisch unterschreiben zu können. Dadurch wird das signierte Dokument vor nachträglicher Veränderung geschützt.

Unsere Leistung
Durch den Betrieb von öffentlich vertrauenswürdigen Public-Key-Infrastrukturen (PKI) stellt D-Trust die notwendigen digitalen Zertifikate zur Verfügung.

Der Managed PKI Service (Certificate Service Manager) der D-Trust erlaubt dabei über Standardschnittstellen die Integration in beispielsweise E-Mail-Gateways oder andere bestehende Infrastrukturen und Systeme.

So können Zertifikate einfach beantragt, verwaltet und manuell oder automatisiert bezogen werden. Verzeichnis- und Verifikationsdienste ermöglichen es Ihnen dann, die Gültigkeit von Zertifikaten sofort zu überprüfen. Dadurch ist eine sichere und vertrauenswürdige Kommunikation im digitalen Zeitalter sichergestellt.

D-Trust ist Ihr Partner, wenn es um Zertifikatsprodukte und eIDAS-konforme qualifizierte Vertrauensdienste geht. Als unabhängige dritte Instanz stellt D-Trust rechtssichere und zertifizierte Vertrauensdienste zur Verfügung, die den höchsten Sicherheitsstandards einer modernen Infrastruktur gemäß ISO-27001- und TÜV-TSI-Level-3-Zertifizierung entsprechen.

Warum Zertifikate von D-Trust?
- **Akzeptiert** – unsere Zertifikate werden von allen gängigen Browsern, E-Mail-Clients und Betriebssystemen unterstützt
- **Umfangreich** – breites Zertifikatsportfolio für alle Anwendungsfälle
- **Effizient** – dank dem Certificate Service Manager (CSM) dauert der Zertifikatsantrag nur wenige Augenblicke
- **Übersichtlich** – zentrale Verwaltung des gesamten Zertifikatsbestands durch maximale Kostenkontrolle

Die Schutzziele der E-Mail-Verschlüsselung

Vertraulichkeit
Der Inhalt von E-Mails kann nur von berechtigten Personen gelesen werden.

Authentizität und Verbindlichkeit
Die Nachricht stammt tatsächlich vom angegebenen Absender.

Integrität
Der Inhalt von E-Mails ist vollständig und unverändert.

D-Trust GmbH | Kommandantenstraße 15 | 10969 Berlin
Tel: +49 (0)30 25 93 91-0 | info@d-trust.net | www.d-trust.net