Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Digitale Signatur als Schlüssel zu sicherer E-Mail-Kommunikation

Positionspapier

2026

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 310
E-Mail: info@teletrust.de
https://www.teletrust.de

© 2026 TeleTrusT

Inhaltsverzeichnis

1 Ausgangslage 4

2 Hemmnisse 4

3 Die digitale Signatur als erster Schritt 4

4 Handlungsempfehlungen 5
4.1 Beiträge des BSI und der öffentlichen Verwaltung 5
4.2 Beiträge der Industrie 5

5 Gemeinsame Initiative 5

6 Fazit 6

1 Ausgangslage

E-Mail ist weiterhin das wichtigste offene Kommunikationsmedium für Wirtschaft, Verwaltung und Gesellschaft. Gleichzeitig gehört sie zu den am häufigsten missbrauchten Kommunikationswegen. Phishing, Identitätsmissbrauch und manipulierte E-Mails verursachen jährlich erhebliche Schäden.

Seit rund 30 Jahren stehen mit S/MIME und OpenPGP international etablierte Verfahren für digitale Signaturen und Ende-zu-Ende-Verschlüsselung zur Verfügung. Dennoch werden diese Verfahren heute nur in sehr geringem Umfang eingesetzt.

Aus Sicht des TeleTrusT-AK "Mail Security" liegt dies nicht an fehlender technischer Reife, sondern an einer Kombination aus organisatorischen, wirtschaftlichen und benutzerbezogenen Hemmnissen.

2 Hemmnisse

Die geringe Verbreitung digitaler Signaturen und verschlüsselter E-Mails hat mehrere Ursachen:

- Persönliche Zertifikate sind für viele Anwender noch immer zu aufwendig zu beschaffen, zu verwalten und regelmäßig zu erneuern.
- Für viele Privatnutzer ist der Nutzen digitaler Signaturen und Verschlüsselung nicht ausreichend sichtbar.
- Für verschlüsselte Kommunikation muss der öffentliche Schlüssel des Kommunikationspartners verfügbar sein. Solange nur wenige Personen über Zertifikate verfügen, bleibt dieser Netzwerkeffekt aus.
- Die Unterstützung in Mail-Programmen und mobilen Endgeräten ist uneinheitlich und häufig nicht benutzerfreundlich.
- (Privat)Nutzer sind mit Schlüsselmanagement (Erstellung, Verteilung, Nutzung, Erneuerung, etc.) und der Unterscheidung von privatem und öffentlichem Schlüssel häufig überfordert.
- Veränderungen einer E-Mail, die nach dem Aufbringen der Signatur durch Gateways oder Mailserver vorgenommen werden, machen digitale Signaturen ungültig.
- Viele Anwender kennen die Möglichkeiten moderner E-Mail-Sicherheit nicht oder empfinden deren Nutzung als zu komplex.
- Organisationen setzen häufig ausschließlich auf Transportverschlüsselung (TLS) oder proprietäre Kommunikationsplattformen und verzichten deshalb auf interoperable Ende-zu-Ende-Verfahren.

3 Die digitale Signatur als erster Schritt

Der TeleTrusT-AK "Mail Security" empfiehlt, die Förderung digitaler Signaturen zunächst in den Mittelpunkt aller Maßnahmen zu stellen.

Digitale Signaturen bieten bereits ohne Verschlüsselung einen unmittelbaren Sicherheitsgewinn. Sie ermöglichen dem Empfänger die Prüfung von Herkunft und Integrität einer E-Mail und erschweren Phishing- und Spoofing-Angriffe erheblich. Gleichzeitig wird mit jeder signierten E-Mail automatisch der öffentliche Schlüssel des Absenders verbreitet. Damit entsteht schrittweise die Voraussetzung für eine spätere Ende-zu-Ende-Verschlüsselung.

Eine flächendeckende Nutzung digitaler Signaturen schafft somit sowohl einen unmittelbaren Sicherheitsnutzen als auch die infrastrukturelle Grundlage für eine breite Nutzung verschlüsselter E-Mail-Kommunikation.

4 Handlungsempfehlungen

4.1 Beiträge des BSI und der öffentlichen Verwaltung

Der öffentliche Sektor sollte eine Vorreiterrolle übernehmen.

Der TeleTrusT-AK "Mail Security" empfiehlt insbesondere:

- Behörden des Bundes und möglichst auch der Länder und Kommunen sollten standardmäßig alle ausgehenden E-Mails digital signieren.
- Die öffentliche Verwaltung sollte digitale Signaturen bei der elektronischen Kommunikation als Regelfall etablieren und damit eine Vorbildfunktion übernehmen.
- Das BSI sollte hierfür technische Leitfäden, Referenzarchitekturen und Musterkonfigurationen bereitstellen.
- Informationskampagnen sollten den Nutzen digitaler Signaturen für den Schutz vor Phishing und Identitätsmissbrauch stärker vermitteln.
- Es sollte ein einfach nutzbares, möglichst kostenfreies Angebot für persönliche E-Mail-Zertifikate gefördert werden. Für die meisten Anwendungsfälle genügt eine zuverlässige Verifikation der E-Mail-Adresse.
- Eine offene Infrastruktur für die Veröffentlichung und den Abruf öffentlicher Schlüssel sollte mit Unterstützung des BSI aufgebaut werden.
- Das BSI sollte Interoperabilitätstests zwischen Mailclients, Mailservern und Sicherheits-Gateways koordinieren und Mindestanforderungen an die korrekte Verarbeitung signierter E-Mails definieren.

4.2 Beiträge der Industrie

Software-Hersteller, Cloud-Anbieter, Trust Service Provider und Betreiber von E-Mail-Infrastrukturen sollten die Nutzung kryptographischer Verfahren deutlich vereinfachen.

Hierzu gehören insbesondere:

- Digitale Signaturen sollten standardmäßig aktiviert oder dem Anwender leicht nutzbar angeboten werden.
- Ausstellung, Erneuerung und Verwaltung von Zertifikaten sollten weitgehend automatisiert erfolgen.
- Öffentliche Schlüssel sollten automatisch veröffentlicht und leicht auffindbar sein.
- Alle relevanten Plattformen (Desktop, Web und Mobilgeräte) sollten eine einheitliche und vollständige Unterstützung bieten.
- Mailserver und Sicherheits-Gateways sollten signierte Nachrichten unverändert transportieren und Veränderungen unterlassen, die eine Signatur ungültig machen.
- Hersteller sollten offene Standards konsequent interoperabel umsetzen und dabei auch Aktualisierungen und Ergänzungen des Standards fortlaufend berücksichtigen.

5 Gemeinsame Initiative

Die Förderung sicherer E-Mail-Kommunikation kann nur als gemeinsame Aufgabe von Staat, Wirtschaft und Standardisierung erfolgreich sein.

Der TeleTrusT-AK "Mail Security" schlägt daher eine koordinierte Initiative unter Beteiligung des BSI, der öffentlichen Verwaltung, der Industrie, der Trust Service Provider sowie der Standardisierungsorganisationen vor. Ziel sollte sein,

- digitale Signaturen als Standard für ausgehende E-Mails zu etablieren,
- den Bezug und die Nutzung von Zertifikaten deutlich zu vereinfachen,
- die Interoperabilität zwischen allen beteiligten Systemen sicherzustellen und
- dadurch die Voraussetzungen für eine spätere flächendeckende Ende-zu-Ende-Verschlüsselung zu schaffen.

6 Fazit

Die Technik für sichere E-Mail-Kommunikation ist seit Jahrzehnten verfügbar. Die entscheidenden Herausforderungen liegen heute nicht mehr in der Kryptographie, sondern in Benutzerfreundlichkeit, Interoperabilität und Verbreitung.

Sichere E-Mail-Kommunikation sollte denselben Grad an Selbstverständlichkeit erreichen wie die Transportverschlüsselung im Web: Milliarden Menschen nutzen täglich das Schloss-Symbol im Browser, ohne über Zertifikate nachzudenken. Diesen Grad an Transparenz muss auch die digitale Signatur erreichen - Ausstellung, Verwaltung, Veröffentlichung, Erneuerung und Nutzung der Zertifikate müssen für den Anwender vollständig automatisiert und unsichtbar ablaufen.

Der TeleTrusT-AK "Mail Security" empfiehlt daher einen pragmatischen, stufenweisen Ansatz: Zunächst sollten digitale Signaturen zum Regelfall werden. Dadurch werden Authentizität und Integrität elektronischer Kommunikation erheblich verbessert und gleichzeitig die notwendige Vertrauensinfrastruktur für eine breite Nutzung der Ende-zu-Ende-Verschlüsselung geschaffen. Dafür sollen ausschließlich offene Standards verwendet werden, um nicht zuletzt den Anforderungen an digitale Souveränität gerecht werden zu können.

Die breite Nutzung digitaler Signaturen ist der wichtigste erste Schritt auf dem Weg zu einer nachhaltig sicheren E-Mail-Kommunikation und liefert damit einen wichtigen Beitrag zur Cybernation Deutschland.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.



Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.