

Transport Layer Security

Verschlüsselung (kurz: TLS) im externen E-Mailverkehr der DRV

Ab dem 07.01.2026 wird die Deutsche Rentenversicherung (DRV) ihren ausgehenden E-Mail-Verkehr auf zwingende TLS-Verschlüsselung umstellen. Der E-Mail-Austausch mit der DRV wird damit nur noch möglich sein, sofern auf der Partnerseite TLS unterstützt wird.

Betreiber von Domänen sollten somit entsprechende Maßnahmen ergreifen bzw. Kontakt mit Ihren IT-Dienstleistern aufnehmen.

Es wurden sämtliche Mailempfänger informiert, bei denen es in den vergangenen 3 Monaten im ausgehenden Mailverkehr zu TLS-Fehlern kam, unabhängig davon, ob TLS nicht oder nur teilweise unterstützt wird.

Die DRV hat keine ausreichenden Ressourcen, um Supportanfragen beantworten zu können.

Aktuell sind bei der DRV folgende TLS-Einstellungen aktiv

Version: TLS v1.2

SSL Cipher(s) to use:

EDH+TLSv1.2:ECDH+TLSv1.2:EDH+HIGH:EDH+MEDIUM:ECDH+HIGH:ECDH+MEDIUM:HIG
aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-
AES256-CCM:!ECDHE-ECDSA-CAMELLIA128-SHA256:!ECDHE-RSA-CAMELLIA128-
SHA256:!ECDHE-ECDSA-CAMELLIA256-SHA384:!ECDHE-RSA-CAMELLIA256-
SHA384:!ECDHE-ECDSA-AES128-CCM:!ECDHE-ECDSA-AES256-CCM

Die Cipher-Einträge sind RegEx...

Erlaubte Cipher

- Cipher mit EDH/ECDH in Kombination mit TLSv1.2
- Cipher mit EDH oder ECDH, die als HIGH oder MEDIUM eingestuft sind
- Generell alle HIGH oder MEDIUM Cipher (wenn nicht anderweitig ausgeschlossen)

nicht erlaubte Cipher

- Schwache Cipher wie: LOW, EXP (Export), RC4, 3DES, SEED, IDEA, MD5, DSS
- Cipher ohne Authentifizierung: aNULL, -aNULL
- Bestimmte konkrete Cipher-Suites, z. B.: DHE-RSA-AES256-SHA, ECDHE-ECDSA-CAMELLIA128-SHA256, ECDHE-ECDSA-AES128-CCM