

TeleTrust-EBCA "PKI-Workshop" 2025

Berlin, 18.09.2025

S/MIME 4.0

Mehr Sicherheit für die E-Mail-Kommunikation

Stefan Cink, Net at Work

- S/MIME = Secure/Multipurpose Internet Mail Extensions
- Standard zur Verschlüsselung und Signierung z.B. von E-Mails, aber auch AS2, AS4 u.a.
- Wird anhand der S/MIME Capabilities ausgehandelt
- Update notwendig wegen neuer Bedrohungen und veralteter Kryptografie

Version	RFC	Jahr	Änderungen
S/MIME 2.0	2311	1998	Einführung von application/pkcs7-mime und multipart/signed, keine IETF-Standardisierung
S/MIME 3.0	2633	1999	CMS als Basis, mehr MIME-Kompatibilität
S/MIME 3.1	3851	2004	Einführung von application/pkcs7-mime für komprimierte Inhalte
S/MIME 3.2	5751	2010	Klarere MIME-Typen, ECC diskutiert aber nicht aufgenommen
S/MIME 4.0	8551	2019	Veraltete Algorithmen entfernt, authentifizierte Verschlüsselung eingefügt, vollständige Ablösung von RFC 5751

Änderungen in S/MIME 4.0 im Detail

- Unterstützung für elliptische Kurven, SHA-2, AES-GCM und ChaCha20-Poly1305
- Bei Verwendung von ECDSA oder ECDH ist NIST P256 verpflichtend zu verwenden.
- SHA-256 oder größer ist **verpflichtend** für Signaturen
- SHA1 ist deprecated
- Authentifizierte Verschlüsselung mit AES-GCM
- Support für internationalized email addresses

Sicherheitsvorteile von S/MIME 4.0

- Authentifizierte Verschlüsselung schützt vor Manipulation, wie z.B. bei EFAIL
- ECC: sicherer bei kürzeren Schlüsseln – ideal für mobile Geräte
- SHA-2: höhere Integrität und Authentizität
- Erfüllt BSI-Anforderungen (TR-03116) auch über 2025 hinaus
- Empfohlen für Behörden, KRITIS, Unternehmen

Der Verbreitungsgrad von S/MIME 4.0

- Gängige E-Mail-Clients wie Outlook, Thunderbird und andere unterstützen es nicht!
- Bei den E-Mail-Gateways gibt es bisher nur einen Anbieter mit S/MIME 4.0 Support
- Eine weitere Mail-Client-Erweiterung eines deutschen Herstellers mit VS-NfD-Zulassung kann es ebenfalls.

Fazit und Empfehlungen

- S/MIME 4.0 = moderner Sicherheitsstandard für E-Mails
- Migration auf SHA-2 dringend notwendig!
- Bestehende Infrastruktur prüfen und aktualisieren, vor allem in regulierten Unternehmen
- Verbreitungsgrad ist äußerst problematisch