

Smart-Mail-Flow API – Änderungen in Version 2.0.0

Smart-Mail-Flow **2.0.0** (15.10.2026) benennt die API-Felder sinnvoll um und ergänzt neue Prüfungen. Die vollständige Beschreibung aller Felder steht auf [Smart-Mail-Flow API](#).

Für Programme, die die API auswerten: Die alten Feldnamen gibt es nicht mehr. Datensätze, die vor der Umstellung eingegangen sind, behalten ihr altes Format. Erkennbar ist das neue Format an `debug.software_version` (`2.0.0` oder höher).

1. Verhalten

Thema	bis 1.x	ab 2.0.0
Test-ID	beliebig	mindestens 8 Zeichen, nur <code>A-Z a-z 0-9 _ -</code> . Sonst wird die Mail beim Einliefern abgewiesen (<code>550 5.1.1 id too short</code> bzw. <code>invalid id</code>). <code>postmaster@</code> und <code>abuse@</code> werden immer angenommen
HTTP-Status der API	immer 200	200 Ergebnis, 400 <code>No token</code> , 404 <code>Token not found</code> , 429 <code>Rate limiter</code> , 500 <code>internal error</code> mit <code>error_id</code>
Kopfzeilen und Betreff	teilweise roh (Zeilenumbrüche, MIME-kodiert)	eine Zeile, dekodiert
TLS 1.2	Warnung auf der Website	gilt als in Ordnung
Spamhaus-Abfragename	Zugangsschlüssel als <code><key></code> (verschwand in HTML-Ansichten, sah aus wie „...“)	<code>[key]</code>

2. Felder im Datensatz (data)

alt	neu
<code>mail_from</code> (enthielt die From-Kopfzeile)	<code>header_from</code>
<code>rcpt_to</code> (enthielt die To-Kopfzeile)	<code>header_to</code>
-	<code>smtp_mail_from</code> , <code>smtp_rcpt_to</code> (SMTP-Umschlag)

3. Felder in debug

alt	neu
analysis_version	entfällt, software_version
client_ip, smtp.source_ip	smtp.client_ip
helo, smtp.helo	smtp.helo
env_sender, smtp_mail_from, smtp.smtp_mail_from, spf_output.envelope_from	smtp.mail_from
smtp.rcpt	smtp.rcpt_to
tls_proto, tls_cipher	smtp.tls.protocol, smtp.tls.cipher (neu: smtp.tls.status)
header_from (Adresse)	header.from[0].address
return_path	header.return_path
spf_output.result/identity/domain/explanation	spf.result/identity/domain/explanation
spf_output.raw_header	mta_checks.spf_header
dkim_status, dkim_detail	dkim.result, dkim.detail
dkim_signatures[]	dkim.signatures[]
dkim_signatures[].algorithm	dkim.signatures[].key_algorithm
dkim_signatures[].rsa_bits	dkim.signatures[].key_bits
dmARC_result	dmARC.result
dmARC.policy	dmARC.published_policy
dmARC.applied_policy	dmARC.effective_policy
envelope_dns	return_path_dns
helo_check (helo, status, addresses, reason)	helo (name, status, addresses, reason)
protocol	ip_protocol
rbl.blacklistmaster	blacklistmaster

4. Neue Felder

- **Allgemein:** checked_at, duration_ms
- **Kopfzeilen:** header.from[] und header.to[] mit address, display_name, display_name_is_address. Dazu header.subject, header.date, header.message_id.
- **SPF:** spf.record (ausgewerteter Eintrag), spf.mechanism (entscheidender Teil), spf.dns_lookups, spf.dns_lookup_limit
- **DKIM je Signatur:**

- canonicalization, signed_headers, body_length_limit
- dns_name, testing
- body_hash_ok, aligned_with_from
- **DMARC:**
 - subdomain_policy, pct, adkim, aspf
 - disposition: was nach DMARC mit dieser Mail geschehen soll, none bei pass
- **ARC (neu):** arc mit status, chain_validation, sealer_trust und instances[]
- **HELO-Teilprüfungen:** helo.syntax, helo.resolves, helo.matches_client_ip
- **Blacklists:** je Liste zusätzlich rcode, resolver, duration_ms. query ist immer vorhanden, null wenn die Liste nicht abgefragt wurde.
- **Domain-Sicherheit (neu):** domain_security der From-Domain mit dnssec, mta_sts, tls_rpt, dane, bimi

5. Entfallen

- analysis_version
- env_sender
- spf_output
- dkim_status, dkim_detail, dkim_signatures (die Spalte dkim_status im Datensatz bleibt)
- dmarc_result
- envelope_dns
- helo_check
- protocol
- rbl
- client_ip, tls_proto, tls_cipher auf oberster Ebene
- dkim_signatures[].rsa_bits (bei ed25519 stand dort "n/a")

Revision #1

Created 15 October 2026 21:20:56 by smartmailflowki

Updated 15 October 2026 21:20:56 by smartmailflowki