

BIMI

Inhaltsverzeichnis

- [1 Funktionsweise](#)
- [2 Typische Einsatzbereiche](#)
- [3 Wichtige Hinweise](#)
- [4 Fazit](#)

BIMI erlaubt Markenlogos neben authentifizierten E-Mails im Posteingang. Voraussetzung sind strenge DMARC-Policy und freigegebene Logo-/Markennachweise.

1 Funktionsweise

Empfangende Mailclients prüfen [DMARC](#)-Pass und laden das freigegebene Markenlogo gemäß BIMI-DNS-Einträgen. So wird sichtbare Marke an authentifizierte Absender gekoppelt.

- **DMARC enforce:** typische Grundvoraussetzung
- **SVG-Logo / Evidence:** Markenfreigabe
- **DNS BIMI-Record:** Verweis auf Logo-Policy

2 Typische Einsatzbereiche

- Markenauftritt in unterstützten Mailclients
- Phishing-Unterscheidung durch sichtbare Authentizität
- Unternehmen mit gereifter E-Mail-Auth

3 Wichtige Hinweise

- Nicht alle Provider zeigen BIMI-Logos.
- [DMARC](#), [DKIM](#)/SPF und Logo-Rechte müssen stimmen.
- Ohne solide Auth bringt BIMI nichts.

4 Fazit

BIMI macht erfolgreiche E-Mail-Authentifizierung sichtbar – ein Branding-Feature auf Basis von [DMARC](#), kein [Spamfilter](#)-Ersatz.