Brand Indicators for Message Identification

Die Grundlage für vertrauenswürdige

E-Mail-Marketing-Kampagnen

Maurice-Jörg Nießen

2025-10-27

Inhaltsverzeichnis

Zielsetzung des “Brand Indicators for Message Identification” 2
Anforderung an die E-Mail-Infrastruktur des Absenders 4
Domain Name System Security Extensions (DNSSEC) 5
Sender Policy Framework (SPF) 7
DomainKeys Identified Mail (DKIM) 9
Domain-based Message Authentication, Reporting & Conformance (DMARC) 11
Anforderungen an das Markenlogo 15
Angepaßtes Design 15
Vektorbasierte Grafik 17
Angepasstes Dateiformat 19
Zertifikat zur Bestätigung der Echtheit der Marke 20
Technische Implementierung 22
Erklärung 24

Zielsetzung des “Brand Indicators for Message Identification”

Die *Brand Indicators for Message Identification* oder kurz *BIMI*, wurde 2019 von einer Koalition aus Unternehmen und Organisationen, der E-Mail- sowie IT- Sicherheits-Branche, entwickelt und die *BIMI Working Group* ins Leben gerufen. Dieser Gruppe haben sich unter anderem folgende Unternehmen angeschlossen:

- *Google*
- *Yahoo (Verizon Media)*
- *Valimail*
- *Proofpoint*
- *Agari*
- *Entrust*
- *Fastmail*

Als gemeinsames Ziel hat sich die Gruppe die Verbesserung der E-Mail-Sicherheit und des Markenschutzes durch offene, standardisierte Lösungen gesetzt.

Obwohl *Microsoft* nicht in der Gruppe vertreten ist und die Clients für *Microsoft Outlook* oder *Office 365* bislang kein *BIMI* unterstützen, decken die unterstützenden E-Mail-Clients einen Großteil des Marktes ab. Eine Studie aus dem Jahr 2023 [1] hat ergeben, dass E-Mails eher mit *Apple Mail* (*64,3%*), *Gmail* (*24,5%*) oder *Yahoo Mail* (*3,0%*) geöffnet werden und zusammen bereits über *90%‘* des Marktes abdecken. Mit *Microsoft Outlook* werden demnach lediglich nur *3,2%* der weltweiten E-Mails geöffnet.

> Technisch bietet *BIMI* selbst keinerlei Massnahmen zur Verbesserung der E-Mail-Sicherheit, sondern setzt auf andere, für die Implementierung erforderliche, Technologien auf.

Für den Empfänger einer E-Mail, der möglicherweise Kunde oder gar potentieller Neukunde ist, erfolgt der Einsatz von *BIMI* sowie der abhängigen Technologien völlig transparent. Um welche Technologien es sich im Einzelnen handelt, wie sie zusammenspielen und was bei ihrer Konfiguration im Zusammenhang mit *BIMI* zu beachten ist, klären wir im nächsten Kapitel.

Doch zuvor beleuchten wir das *“Benutzererlebnis”*[2], besser bekannt als die *“user experience (UX)”*, bei der derzeitigen Nutzung eines E-Mail-Clients sowohl ohne und als auch mit *BIMI*-Unterstützung.

Es wird wohl kaum einen Anwender geben, der noch nie eine *Spam*-, *Phishing*- oder anders geartete *Spoofing*-E-Mail erhalten hat. *Spam*-Filter sollen diese anhand von Filterregeln und Bewertungskriterien

[1] “*Neueste Statistiken und Trends zu E-Mail-Clients 2023*”(Vibetrace, 17.09.2023)
[2] DIN ISO 9241 Teil 210

auf das bestmögliche Minimum reduzieren. Je nach Einstellung landen E-Mails in einem gesonderten Ordner, dem "*Spam-Ordner*", oder dem Betreff der E-Mail wird ein Präfix wie "`[SPAM]`" beigemischt. Jedoch erfolgt eine fehlerhafte Ablage in solche Ordner derart häufig, dass man insbesondere bei einer ersten Kontaktaufnahme, schon vorab darauf hingewiesen wird auch den "*Spam-Ordner*" auf die zu erwartenden E-Mail zu prüfen.

Administratoren agieren bei neuen Technologien meist eher *"zaghaft"*, besonders dann, wenn ihre Einstellungen zu weniger Daten oder gar Datenverlust führen könnten. Die so getroffenen Einstellungen werden erst dann wieder verändert, wenn etwas nicht (mehr) funktioniert oder diese von einem Unabhängigen (möglicherweise bedingt durch einen Audit oder gar einem Vorfall) bewertet werden. Inwieweit die als schon implementiert geglaubte Technologie überhaupt die erhoffte Wirkung entfalten konnte, stellt sich dann im Nachhinein heraus.

> Bei einer serverseitigen Ablehnung (`reject`) einer E-Mail, wird der vermeintliche Empfänger zwar über deren Existenz in völliger Unkenntnis gelassen, aber der Absender wird über die Unzustellbarkeit informiert. Wirklich verloren geht hierbei also nichts, doch geschieht dies in der Regel in 6 bis 48 Stunden nach dem ersten Zustellversuch - damit also weit oberhalb der Geduld oder Erwartungshaltung einiger E-Mail-Empfänger.

Somit werden bei geringsten Zweifeln E-Mails also schlimmstenfalls bunt gemischt nebeneinander in irgendeinem Ordner ohne jegliche weitere Unterscheidung dargestellt, egal ob sie "*false positives*" oder "*very, very true positives*" sind. Ob eine E-Mail überhaupt überprüft wurden und welche Prüfungen dabei erfolgreich waren oder gar fehlgeschlagen sind, ist für den Empfänger der E-Mail erstmal nicht ersichtlich. Diese Informationen stecken in der Regel im *E-Mail-Header*.

Nur einige wenige E-Mails-Clients erlauben die Einfärbung von E-Mails, wenn bestimmte Bestandteile im Kopf der E-Mail und damit in ihren *Meta-Daten* zu finden sind. Bei anderen E-Mail-Clients ist die Anzeige des *E-Mail-Headers* selbst entweder gut in der Menüstruktur versteckt oder sogar gar nicht mehr möglich. Abgesehen von den technischen Fähigkeiten des Empfängers die dort stehenden Informationen auch richtig deuten zu können, ist diese Methode für eine kontinuierliche Überprüfung eingehender E-Mails wenig gebrauchstauglich.

Doch genau an dieser Stelle setzt *BIMI* an. E-Mails, bei denen einerseits die Technologien zur Verbesserung der E-Mail-Sicherheit nicht nur zum Einsatz kamen, sondern auch nichts zu beanstanden hatten, werden mit dem Markenlogo des jeweiligen Absenders versehen, sofern diese *BIMI* implementiert haben.

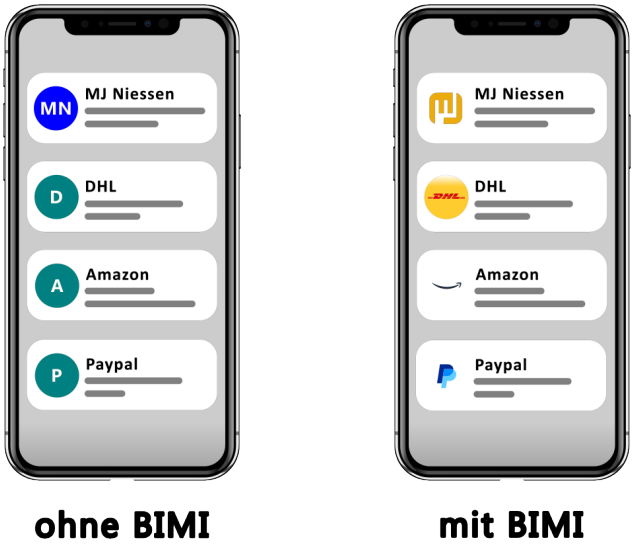

Abbildung 1: E-Mail-Client mit und ohne BIMI

Wie man aus den oben genannten Marktanteilen ableiten kann, werden heute überwiegend E-Mails auf mobilen Endgeräten gelesen oder zumindest entgegengenommen. Die vorab installierten E-Mail-Clients der gängigsten Geräte (iPhone, iPad und Androids) unterstützen bereits *BIMI*.

Eine Unterstützung durch den Absender erhöht nicht nur die E-Mail-Sicherheit auf Seiten der Empfänger, sondern stärkt auch das Vertrauen in entsprechende E-Mails und deren Inhalt. Die Wahrnehmung der Marke wird verbessert, wenn das bekannte Markenlogo neben der E-Mail im Client angezeigt wird. Mögliche Fälschungen können so von Empfängern besser erkannt werden, E-Mails mit Markenlogo werden somit eher geöffnet und bestenfalls auch gelesen.

Vereinfacht zusammengefasst ist *BIMI* das von sozialen Medien bekannte "*verifizierende Häkchen*" für E-Mails, bei dem die jeweilige Marke direkt im E-Mail-Client sichtbar wird, wenn dann alles stimmt.

Anforderung an die E-Mail-Infrastruktur des Absenders

BIMI stellt selbst kein technisches Verfahren zur direkten Verbesserung der E-Mail-Sicherheit bereit, sondern erwartet die wirkungsvolle Konfiguration bereits etablierter Verfahren. Diese existieren bereits seit Jahren, wurden aber teilweise noch nicht oder nicht umfassend von allen Betreibern von E-Mail-Infrastrukturen umgesetzt.

Damit die Echtheit der jeweiligen Marke aber auch ein hohes Sicherheitsniveau durch *BIMI* garantiert werden kann, wird die erfolgreiche Umsetzung folgender Verfahren und Standards auf der Seite des

Absenders vorausgesetzt:

- *Domain Name System Security Extensions (DNSSEC - technisch nicht erforderlich, aber dringend empfohlen)*
- *Sender Policy Framework (SPF)*
- *DomainKeys Identified Mail (DKIM)*
- *Domain-based Message Authentication, Reporting & Conformance (DMARC)*

Im Folgenden gehe ich davon aus, dass diese technischen Voraussetzungen für eine Implementierung von *BIMI* bereits geschaffen wurden. Jedes dieser Verfahren bietet - entsprechend konfiguriert - bereits einen erheblichen Mehrwert für die E-Mail- und Domain-Sicherheit und gilt als irgendwas zwischen *Best-Practice* und *Standard*. Ich gehe allerdings etwas näher auf sie ein, um ihre Rolle und ihr Wirken im Verbund hinsichtlich *BIMI* besser zu verstehen.

Domain Name System Security Extensions (DNSSEC)

Die *Domain Name System Security Extensions (DNSSEC)* stellen eine Erweiterung des *Domain Name System (DNS)* dar, welche bereits 2004 entwickelt [3] wurde. Sie wird heute von mehr als 90% aller *Top-Level-Domains (TLDs)* unterstützt und von über einem Drittel aller Internetbenutzer tagtäglich genutzt.

Aufgrund seiner Funktion wird das *DNS* gerne mal auch als "*Die Gelben Seiten des Internets*" bezeichnet. Auch wenn es wesentlich komplexer ist, liefert es zu einer bestimmten Domain die jeweilige technisch verwertbare IP-Adresse. Bedingt durch die ständig wachsende Anzahl von Internetseiten (geschätzter Zuwachs 10.500 pro Stunde) die von über 1,1 Milliarden Menschen aufgerufen werden, müssen für eine *DNS*-Informationen schnell verfügbar sein. Hierzu werden die Informationen redundant verteilt und von mehreren Instanzen temporär zwischenspeichert. Man erhält daher in den seltensten Fällen seine Antwort direkt von einem für die Domain autorisierten *DNS*-Server selbst, sondern wahrscheinlich eher von einem der dazwischen geschalteten *Cache*-Server.

DNSSEC sorgt nun dafür, dass es hierbei nicht wie bei dem Kinderspiel "*Die stille Post*" zugeht und man anderen Ende der Kette gegebenenfalls eine gänzlich andere Information erhält als der Domaininhaber vorgesehen hat. Es stellt hierbei die *Integrität* und *Authentizität* der *DNS*-Daten sicher, sodass diese über digitale Signaturen auf möglicherweise unterwegs vorgenommene Manipulationen an jedem Punkt der Kette geprüft werden können. Einen Schutz der *Vertraulichkeit*, durch beispielsweise eine Verschlüsselung der Anfrage und der Informationen selbst, gewährleistet *DNSSEC* selbst nicht. Dies übernehmen bei speziellem Bedarf Technologien wie *DNS over HTTPS (DoH)* oder *DNS over TLS (DoT)*.

Durch Manipulationen der *DNS*-Daten könnten Cyberkriminelle beispielsweise in die Kommunikation mogeln ("*man in the middle*") oder ihre Opfer auf andere Hosts umleiten ("*DNS spoofing*"). Besonders

[3] RFC3833 - "*Threat Analysis of the Domain Name System (DNS)*"

in der Lockdown-Phase von Corona wurden so zahlreiche im "*Home-Office*" arbeitende Mitarbeiter auf andere, nicht zu ihrer Firma gehörende *VPN*-Server ("*virtual private network*") umgeleitet, um an ihre Zugangsdaten zu gelangen[4] [5].

Doch auch Internet-Provider (ISPs) manipulieren gerne mal *DNS*-Daten für unterschiedliche Zwecke. So war es lange Zeit üblich, bei der Eingabe einer falschen oder ungültigen Domain statt einem Fehler (`NXDOMAIN`) den Nutzer auf eine eigene Werbeseite weiterzuleiten. Um nicht einen Verlust an Netzneutralität, einen generellen Vertrauensverlust oder gar Probleme mit dem Datenschutz zu riskieren, haben zumindest hierzulande die *ISP*s davon größtenteils abgesehen. In anderen Länder wird unter anderem auf diese Weise die Zensur politischer Inhalte oder "*unerwünschter*" Webseiten bewerkstelligt.

> Der Vollständigkeit halber sei aber auch erwähnt, dass es auch technisch gewollte Manipulationen am *DNS*-Daten stattfinden, um zum Beispiel den Zugriff auf *Content-Delivery-Netzwerke (CDN)* auf geolokalisierte Server umzuleiten, um die Ladezeiten der Inhalte zu optimieren. Als bekannte *CDN* wären hier beispielsweise *Cloudflare*, *Akamai*, *Amazon CloudFront*, *Google Cloud CDN* oder *Microsoft Azure CDN* zu nennen. Diese verzichten entweder auf den gänzlich auf Einsatz von *DNSSEC* oder implementieren etwas aufwändigere Lösungen.

Mittlerweile werden aber auch weitaus sensiblere Daten als nur IP-Adressen mittels *DNS* in Verbindung mit der jeweiligen Domain öffentlich bereitgestellt. Zu nennen wären hier beispielsweise öffentliche Schlüssel von Servern, Webseiten oder administrativen Zugängen, digitale Fingerabdrücke von Dateien oder Programmen, Versionsnummer von Sicherheitssoftware oder Schlüssel zur Beglaubigung des Besitzes einer Domain gegenüber Dritten. Im Grunde genommen alles Angaben, um andere Informationen in ihrer Echtheit zu bestätigen.

> Ohne die generelle Absicherung der *DNS*-Daten durch *DNSSEC* würden diese zusätzlichen Angaben eine Sicherheit suggerieren, die es so möglicherweise aber gar nicht gibt, da auch diese vermeintliche Bestätigung der Angaben gezielt von Cyberkriminellen manipuliert werden könnte.

> Für den sinnvollen Einsatz von *BIMI* - und damit indirekt auch *SPF*, *DKIM* sowie *DMARC* - wird daher die Unterstützung von *DNSSEC* **dringend empfohlen**.

[4] "*Hackers Using COVID-19 Phishing, Website Spoofing for Credential Theft*" (TechTarget, 20.05.2020)
[5] "*Experts Detect 30,000% Increase in #COVID19 Threats*" (Infosecurity Magazine, 27.04.2020)

Sender Policy Framework (SPF)

Das bereits schon in 2014 entworfene *Sender Policy Framework*[6] soll das Fälschen von E-Mail-Adressen verhindern, in dem es das Versenden von nicht legitimierten *Mail Transfer Agents (MTA)* unterbindet. Ein *MTA* ist als E- Mail-Server zu verstehen, welcher E-Mails entgegen nimmt und an einen für die Empfängeradresse zuständigen E-Mail-Server weiterleitet. Ein *Mail Exchanger (MX)* nimmt hingegen nur E-Mails für eine oder von bestimmten Domains entgegen.

> Verglichen zu einem Brief in Papierform, lässt sich vereinfacht sagen, dass der *MX* die Rolle des lokalen Briefträgers und der *MTA* die Rolle eines Verteilerzentrums übernimmt. Die Überprüfung der auf Briefumschlag hinterlegten Angaben käme hierbei der Rolle von *SPF* gleich.

Als Faustregel gilt, dass ein einzelner Server - egal ob nun als *MTA* oder *MX* eingesetzt - je nach Hardware, Optimierung und Reputation durchaus 100.000 bis 300.000 E-Mails pro Tag vermitteln kann. Für die E-Mail-Nutzung der meisten Domains existiert somit ein zweiter E-Mail-Server nur für den Fall eines Ausfalles oder Wartung des ersten und weniger um die Flut an E-Mails bewältigen zu können.

Hierzu verwendet *SPF* einen im *Domain Name System (DNS)* der Domain hinterlegten TXT-Eintrag[7], welcher die IP-Adressen aller legitimierten *MTA* enthält und dort auch regelt wie mit nicht aufgeführten *MTA* umzugehen ist. Bei der Entgegennahme einer E-Mail wird die Legitimation überprüft und entsprechend verfahren.

```
mjniessen.com IN TXT "v=spf1 include:spf.google.com
↪  include:spf.microsoft.com include:amazonses.com ip4:5.45.109.126
↪  ip6:2a03:4000:6:2381:144b:df2a:cacc:29d1/64 ~all"
```

Anders als bei den TXT-Einträgen der noch folgenden Verfahren werden hier die Angaben mit Leerzeichen voneinander getrennt und keine Semikola verwendet. Der obenstehende, exemplarische *SPF*-Eintrag bewirkt, dass nicht nur ein *MTA*, welcher hier mit seinen IP-Adressen (Version 4 und 6) als Versender angegeben wurde, sondern auch zahlreiche andere Hosts gängiger Cloudanbieter als mögliche Versender legitimiert wurden. Das unscheinbare **`all`** mit einer vorgestellten Tilde (**~**) am Ende des Eintrages rundet dieses als Negativ-Beispiel zu verstehenden *SPF*-Eintrag nur noch ab.

Leider sind derartige Einträge auch im produktiven Einsatz keine Seltenheit. Möglicherweise hat man die reservierten Beispiele aus irgendwelchen Anleitungen einfach übernommen und später den Eintrag um weitere exemplarische Umsetzungen der neuen Anforderung erweitert, ohne die Sinnhaftigkeit des

[6] `RFC7208` - *"Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1"*
[7] `RFC1035` - *"Domain Names - Implementation and Specification"*

dadurch entstehenden gesamten Eintrages infrage zu stellen. Gerne werden von E-Mail- Dienstleister, die ihre Infrastruktur in einer Cloud betreiben lassen, alle nur erdenklich möglichen IP-Adressen in einen solchen Eintrag gepackt. Damit spart er sich zwar kundenspezifischen Konfigurationsaufwand, aber dies auf Kosten der E-Mail-Sicherheit des jeweiligen Kunden.

Durch das bereits erwähnte **`~all`** am Ende wird des *SPF*-Eintrages, wird ein sogenanntes "*soft failure*" definiert. Hierbei wird zwar eine Warnung im Header der E-Mail generiert, wenn eine E-Mail von einem nicht legitimierten Host versendet wird, aber die E-Mail dennoch zugestellt oder nicht obliegt der Konfiguration des verarbeitenden E-Mail-Servers und dem Ergebnis wohl möglicher weiterer Prüfungen. Im besten Fall wird sie in einen gesonderten Ordner sortiert, wodurch sich das anfangs beschriebene, einleitende Szenario ergibt.

Noch fataler wäre im Übrigen ein **`+all`**, welches nicht ein "*Plus*" an Sicherheit bietet, sondern in jedem Fall die jeweilige IP-Adresse als legitimen Versender für die Domain ausweist.

Zum Schutz vor gefälschten Absendern sollte grundsätzlich die Einstellung *"hard failure"* gesetzt werden. Dies lässt sich mit **`-all`** - also einem Minus statt der Tilde oder dem Plus - bewerkstelligen. So werden E-Mails von für die jeweilige Domain nicht legitimierten E-Mail-Servern abgelehnt - idealerweise noch bevor sie den "*lokalen Briefträger*" erreichen. Wie bereits erwähnt, wird der Absender der E-Mail in der Regel über die Unzustellbarkeit der E-Mail informiert.

```
Message delivery failed.
Recipient Name: nonexist@mjniessen.com
Recipient Domain: mjniessen.com
Error Message: 550 5.7.1 Relaying denied

SMTP Error Code 550:
Relaying denied
```

Die im *SPF*-Eintrag enthaltenen **`include`**-Anweisungen sind so zu verstehen, dass die hinterlegte Domain ebenfalls abgefragt und auf eine entsprechende Übereinstimmung bei Eingang einer E-Mail überprüft wird. Der hinterlegte *SPF*-Eintrag kann abermals ein oder gar mehrere **`include`**-Anweisungen enthalten und somit bildet sich möglicherweise schnell eine recht umfangreiche Liste von IP-Adressen, die technisch nach *SPF* im Namen der Domain E-Mails versenden dürfen.

Mir sind schon mehrfach *SPF*-Einträge begegnet, in denen die dort definierten als Versender infrage kommende *MTAs*, zahlenmäßig um ein Vielfaches die Anzahl der auf den Kontinenten überhaupt verfügbaren, relevanten E-Mail-Server überstieg.

Je mehr mögliche Hosts gelistet sind, desto leichter wird es einem Cyberkriminellen gemacht an einen passenden Host zu gelangen, um unberechtigt E-Mails mit gefälschten Absendern zu versenden.

Im oben genannten (schlechten) Beispiel hat er sogar die Wahl, über welchen Cloudanbieter er mittels eines (Test-)Account seine *Phishing*-, *Spoof*- oder gar *Spam*-Mails loswird. Zwar sperren die Cloudanbieter den üblichen Port (*TCP/25*) für eine direkte, nicht über ihre E-Mail-Infrastruktur laufende, Kommunikation mit externen E-Mail-Servern, doch über alternative Ports ist es in der Regel weiterhin möglich. Solange die Absender-*IP* gelistet ist, werden SPF-Überprüfungen bei den jeweiligen Empfängern nicht zu beanstanden haben und seine E-Mails (ohne weitere Überprüfungen, wie z.B. *DKIM*) zugestellt werden. Ab da obliegt es meist den Empfängern, ob sie auf die Fälschungen hereinfallen oder nicht. Dank des Einsatzes von KI, gelingt es Cyberkriminellen mittlerweile Fälschungen zu generieren, die inhaltlich "*echter*" wirken als so manche Originale. Man tut also gut daran, die Liste so klein wie nur möglich zu halten.

DomainKeys Identified Mail (DKIM)

DKIM ist ein in 2011 entwickeltes Verfahren[8], bei dem ausgehende E-Mails mit einer digitalen Signatur versehen werden, die über *DNS* veröffentlichten öffentlichen Schlüssel validiert werden kann.

Getrennt voneinander werden der Inhalt selbst und bestimmte Kopfzeilen der E-Mail signiert und der *DKIM*-Signatur hinzugefügt. Hierbei handelt es sich in der Regel um Kopfzeilen wie `From`, `To`, `Date`, `Subject`, `Message-ID` oder `MIME-Version`, welche typischerweise nur beim Erstellen einer E-Mail dieser auch hinzugefügt werden. Kopfzeilen wie `Received`, `Return-Path` oder `Delivered-To` werden nicht signiert, da sie sich auf dem Transportweg verändern oder erst später hinzugefügt werden können.

Sobald an den signierten Kopfzeilen oder dem Inhalt der E-Mail Änderungen vorgenommen oder gar Teile entfernt werden, stimmt die hinterlegte digitale Signatur nicht mehr und die *DKIM*-Prüfung schlägt fehl.

```
DKIM-Signature: v=1; a=rsa-sha256; d=mjniessen.com; s=dkim-20241208;
     c=relaxed/simple; q=dns/txt; i=test@mjniessen.com;
     t=1751946431; x=1751030632; l=200;
     h=from:to:subject:date:keywords:keywords;
     z=From:test@mjniessen.com|To:du@hohlhupe.de|
       Subject:demo=20run|Date:July=208,=202505=208:47:11=20PM=20-0700;
     bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
     b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
             VoG4ZHRNiYzR
```

Die exemplarische *DKIM*-Signatur der Absenderdomain **`mjniessen.com`** enthält unter dem dem Tag

[8] `RFC6378` - "*DomainKeys Identified Mail (DKIM) Signatures*"

b= die *Base64*-codierte, digitale Signatur des Inhaltes der an **du@hohlhupe.de** gerichteten E-Mail. Analog dazu sind die unter dem Tag **h=** aufgeführten Kopfzeilen unter **bh=** enthalten.

Das Tag **s=** enthält den sogenannten *DKIM-Selector* (hier: **dkim-20241208**) und stellt den Bezug zu einer im *DNS* der Absenderdomain hinterlegten Information her, welche zur Erstellung und Überprüfung der digitalen Signatur mittels eines bestimmten kryptografischen Verfahrens (**a=**) herangezogen wird.

```
dkim-20241208._domainkey.mjniessen.com IN TXT "v=DKIM1; p=76E629F05F70
↪  9EF665853333 EEC3F5ADE69A 2362BECE4065 8267AB2FC3CB 6CBE"
```

Zeitgleich lassen sich von einer Absenderdomain auch mehrere, unterschiedliche *DKIM-Selector* verwenden, solange der für den jeweils hinterlegten Selektor verwendete, kryptografische Schlüssel auch unter **[DKIM-Selector]._domainkey.[Domain]** im *DNS* hinterlegt ist.

> Wenn man auf die Wiederverwendung eines *DKIM-Selectors* verzichtet und alte Schlüssel im *DNS* belässt, lassen sich auch noch Jahre später E-Mails anhand der damals verwendeten Schlüssel überprüfen. Wurde dem *Selector* (beispielsweise `default`) allerdings bereits ein anderer, neuerer Schlüssel zugewiesen, kann der Empfänger die damalige E-Mails nicht mehr hinsichtlich ihrer Validität mittels *DKIM* überprüfen.

Um die Funktion von *DKIM* analog für einen postalischen Brief darzustellen, muss man sich einerseits ein auf den Briefumschlag angebrachtes Siegel vorstellen, welches beim Öffnen des Briefes zerstört wird (Schutzziel: *Integrität*). Andererseits wird zusätzlich noch die (grobe) Herkunft des Briefes, durch beispielsweise ein in Wachs gepresstes Wappen eines Siegelrings oder einem modernen QR-Code, bestätigt (Schutzziel: *Authentizität*).

Die Aussage, dass der Inhalt einer E-Mail durch *DKIM* geschützt sei, bezieht sich alleinig auf den Schutz vor möglichen Manipulationen ausgehend vom jeweiligen signierenden E-Mail-Server. Eine Verschlüsselung des Inhaltes (Schutzziel: *Vertraulichkeit*) findet mit *DKIM* nicht statt.

Für einen *Ende-zu-Ende-Schutz* (oder besser *Absender-zu-Empfänger-Schutz*) wird eine sehr ähnliche Signatur mittels beispielsweise *S/MIME* oder *PGP* benötigt.

> Viele Unternehmungen statten ihre Mitarbeiter zwar mit den hierzu erforderlichen, personenbezogenen E-Mail-Zertifikaten aus, forcieren aber nicht deren Nutzung. Stattdessen wird die Einhaltung hinsichtlich des "*Corporate Design*" zur Wiedererkennung verschärft, doch Design lassen sich schnell und einfach kopieren.

In einem geschäftlichen Kontext sollte wirklich **jede E-Mail** von seinem Absender persönlich **signiert** sein, damit Empfänger einerseits die *Authentizität* und damit auch die *Verbindlichkeit* des Inhaltes überprüfen können, aber andererseits so auch einen öffentlichen Schlüssel erhalten, um bei Bedarf sensible Daten in **verschlüsselter Form** mit dem Absender **direkt austauschen** zu können.

Viele Spam-Filter oder Gateways fügen dem Betreff von eingehenden E-Mails Präfixe wie beispielsweise `[SPAM]`, `[VIRUS]`, `[INTERNAL]` oder `[MARKETING]` hinzu, um den Empfänger mit zusätzlichen Informationen bezüglich der jeweiligen E-Mail zu versorgen. Hierdurch wird *DKIM* meist unbeabsichtigt gebrochen. Mittels einer weiteren, in diesem Dokument aber nicht näher behandelten Technologie namens *Authenticated Received Chain* (*ARC*), ließe sich dies kombinieren.

Für die in diesem Dokument thematisierte Umsetzung von *BIMI* müssen **alle** ausgehenden E-Mails der entsprechenden, versendenden Domain mit einer *DKIM*-Signatur versehen werden. Ohne eine solche **gültige** und **überprüfbare** Signatur wird *BIMI* kein Markenlogo zu der E-Mail anzeigen. Hierzu sind möglicherweise noch weitere Konfigurationen oder gar Installationen an dem jeweiligen E-Mails-Server vorzunehmen.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

Domain-based Message Authentication, Reporting & Conformance (DMARC) wurde in 2015 [9] entwickelt und baut auf *SPF* sowie *DKIM* auf. Mit *DMARC* können Richtlinien (engl. *policies*) festgelegt werden, wie E-Mail-Server mit E-Mails der entsprechenden Domain umgehen sollen, bei denen die *DKIM*- und/oder *SPF*-Prüfung fehlschlägt.

Verglichen mit der Zustellung eines Briefes, gleicht *DMARC* der empfohlenen Richtlinie oder Arbeitsanweisung für die Postboten (*MTA*), wie mit Briefen umgegangen werden soll, wenn etwas mit den auf dem Umschlag hinterlegten Daten oder der Sendung selbst nicht stimmt - wie zum Beispiel die Rücksendung an den Absender.

Die in der *DMARC*-Spezifikation noch vorgesehene Option, in einem solchen Fall gar nichts zu tun (**p=none**), sieht *BIMI* grundsätzlich **nicht** vor. Eine derart gesetzte *DMARC*-Policy setzt sämtliche Schutzwirkung außer Kraft und macht nur Sinn, wenn man vor einer Produktivsetzung die Auswirkungen studieren möchte.

[9] `RFC7489` - "*Domain-based Message Authentication, Reporting, and Conformance (DMARC)*"

Deutlich wirksamer wäre eine Richtlinie, welche besagt, dass entsprechende E-Mails in einen gesonderten (Spam-)Ordner (**`p=quarantine`**) einzusortieren oder erst gar nicht anzunehmen (**`p=reject`**) sind.

> Je nach Umsetzung von **`p=quarantine`** auf der Seite des Empfängers, landen E-Mails ohne jegliche weitere, für den Empfänger sichtbare Kennzeichnung direkt neben einwandfrei überprüften E-Mails im selben Eingangspostfach. Hinsichtlich eines sicheren E-Mail-Versands ist daher ein **`p=reject`** zu bevorzugen.

Zusätzlich werden mit *DMARC* Berichtsfunktionen ermöglicht, durch welche die verantwortlichen Domaininhaber Informationen über Fehler oder gar missbräuchlich verwendete E-Mail-Adressen erhalten können. Diese Berichte werden von *DMARC*-unterstützenden E-Mail-Servern in der Regel einmal täglich verfasst und als maschinenlesbare *XML*-Datei an die im *DMARC*-Eintrag der Absenderdomain hinterlegte E-Mail-Adresse (**`rua=`**) verschickt.

```
<feedback>
  <report_metadata>
    <org_name>hohlhupe.de</org_name>
    <email>dmarc-reports@hohlhupe.de</email>
    <report_id>20250708-001</report_id>
    <date_range>
      <begin>1751913600</begin>
      <end>1752000000</end>
    </date_range>
  </report_metadata>

  <policy_published>
    <domain>hohlhupe.de</domain>
    <adkim>s</adkim>
    <aspf>s</aspf>
    <p>reject</p>
    <sp>reject</sp>
    <pct>100</pct>
  </policy_published>

  <record>
    <row>
      <source_ip>37.221.192.123</source_ip>
      <count>23</count>
      <policy_evaluated>
        <disposition>reject</disposition>
```

```
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>

    <identifiers>
      <header_from>mjniessen.com</header_from>
    </identifiers>

    <auth_results>
      <dkim>
        <domain>mjniessen.com</domain>
        <result>fail</result>
      </dkim>
      <spf>
        <domain>mjniessen.com</domain>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```

Mit etwas Übung lassen sich aus diesen Berichten, auch ohne weitere technische Unterstützung, erforderliche Informationen entnehmen. In dem Beispielbericht wurde am 08.07.2025 (**`1751913600`**) insgesamt **`23`** mal (**`count`**) von der IP-Adresse **`32.221.192.123`** versucht, eine E-Mail im Namen von **`mjniessen.com`** zuzustellen. Aufgrund fehlgeschlagener *DKIM*-Überprüfungen (**`dkim: fail`**) wurden die E-Mails abgelehnt (**`disposition: reject`**). Zusätzlich sind noch Metadaten zum Bericht selbst sowie die zur Auswertung herangezogenen *DMARC*-Einstellungen enthalten.

Mehr Details - insbesondere zu den entsprechenden E-Mails - sind den *aggregierte DMARC-Berichten* nicht zu entnehmen. Anhand der enthaltenen IP-Adresse in Kombination mit dem angegebenen Zeitraum lässt sich feststellen, ob der Zustellversuch aus der eigenen Infrastruktur, von einer möglicherweise zugekauften Dienstleistungen oder doch von irgendeinem fremden Rechner stammt. Optionale *forensische DMARC-Berichte* liefern gegebenenfalls mehr Informationen zu den entsprechenden E-Mails, aber nicht zwingend Informationen die zur Klärung beitragen - sofern solche Berichte überhaupt bereitgestellt werden.

Innerhalb der EU sollte auf die Verwendung der Option sich einen *forensischen Bericht* (**`ruf=`**) zuschicken zu lassen eher verzichtet werden. Je nach Umsetzung anderer Domains erhalten sie ansonsten möglicherweise Inhalte, die nicht für sie bestimmt sind und sie nach der *Datenschutz-Grundverordnung* (*DSGVO*) angreifbar machen.

Bei im Zeitraum von mehreren unterschiedlichen IP-Adressen gesendeten E-Mails wird der Bericht entsprechend erweitert. Je nach Intensität und Betrachtungszeitraum kommen schnell mal mehrere mehrzeilige *XML*-Berichte zusammen, dass man zur gewissenhaften Analyse auf die Unterstützung von Scripts (wie z.B. `dmarc-cat`[10], `dmarc-report-viewer`[11] oder `parsedmarc`[12]) oder gar Dienstleister (wie z.B. *dmarcian*[13], *ActiveCampaign*[14] oder *EasyDMARC*[15]) zurückgreifen muss.

> Jedoch gänzlich auf die Zusendung von Berichten zu verzichten, indem man keine E-Mail-Adresse (**`rua=`**) angibt, ist grundsätzlich nicht zu empfehlen. Möglichen Angreifern würde man so offenkundig signalisieren, dass über einen Missbrauch vorerst niemand Verantwortliches in Kenntnis gesetzt wird.

Um einen eigenen E-Mail-Server ebenfalls das Versenden von *DMARC*-Berichten für eingehende E-Mails von *DMARC*-unterstützenden Domains beizubringen, sind weitere Konfigurationen oder gar Installationen erforderlich. Für die *BIMI*-Implementierung sind jedoch nur die ausgehende E-Mails der eigenen Domains relevant.

Das in der *DMARC*-Richtlinie ausgedrückte, gewünschte Verhalten wird ähnlich wie bei *SPF* oder *DKIM* ebenfalls über einen im *DNS* der jeweiligen Domain hinterlegten TXT-Eintrag "*gesteuert*". Grundsätzlich handelt es sich vielmehr um eine "*Bitte um Berücksichtigung*", denn unterstützt der empfangende E-Mail-Server *DMARC* nicht oder ist völlig konträr zu dem gewünschten Verhalten konfiguriert, ist in diesem speziellen Fall nicht mit einer "*steuernden*" Wirkung des eigenen *DMARC*-Eintrages zu rechnen. Da wir an dieser Stelle allerdings von einem *BIMI*-unterstützenden E-Mail-Client auf der Empfängerseite ausgehen, wird dieser zumindest dahingehend *DMARC* überprüfen, um festzustellen ob die Voraussetzungen zur Darstellung des Markenlogos gegeben sind oder nicht.

```
_dmarc.mjniessen.com.  IN  TXT  "v=DMARC1; p=reject; fo=1;
↪  rua=mailto:dmarc@mjniessen.com"
```

Dieser *DMARC*-Eintrag ist zwar *BIMI*-konform, aber eher als exemplarische Ausgangskonfiguration zu verstehen. Um die Bedürfnisse der jeweiligen Domain abdecken zu können, sind gegebenenfalls noch entsprechende Anpassungen notwendig. So sollten beispielsweise auch entsprechende Policies für nicht genutzte Subdomains gesetzt werden.[16]

[10] Github - `keltia/dmarc-cat`
[11] Github - `cry-inc/dmarc-report-viewer`
[12] Github - `domainaware/parsedmarc`
[13] dmarcian
[14] ActiveCampaign
[15] EasyDMARC
[16] "*Kein Einfallstor für Phishing: SPF & DMARC für Subdomains*" (Maurice-Jörg Nießen)

> Mittels des im Beispiel vorhandenem **`fo=1`** lässt sich ein Bericht bereits anfordern, sobald eine Überprüfung durch *SPF* **oder** *DKIM* fehlschlägt. Standardmäßig geschieht dies erst, wenn **beide** Überprüfungen fehlschlagen, also der Absender zweifelhaft ist **und** eine Manipulation (oder kein *DKIM*) vorliegt.

Mit Blick auf die zunehmende Zahl von Fällen, bei denen Unternehmen aufgrund einem in die Jahre gekommenem Stand ihrer E-Mail- und DNS-Sicherheit zu Schadensersatzleistungen gemäß *§ 82 DSGVO* verurteilt wurden, sollte man eine restriktiv formulierte *DMARC*-Richtlinie vielleicht auch mal als eine klare Ansage im folgendem Sinne verstehen:

Wenn ihr aber trotz fehlgeschlagener Prüfung mittels SPF, DKIM, DMARC oder DNSSEC mit offensichtlich nicht von uns stammenden E-Mails arbeitet, dann liegt es nicht an uns!

Anforderungen an das Markenlogo

Damit man die eigene Marke innerhalb der E-Mail-Kommunikation mit *BIMI* für die Empfänger sichtbar wird, benötigt man natürlich erstmal ein Logo in digitaler Form.

> Doch bevor wir uns hinsichtlich des richtigen Dateiformates Gedanken machen oder gar schon die damals von einer Agentur erstellte Datei der IT zur "*technischen Umsetzung*" überlassen, sind **zuvor** noch ein paar **Design-Entscheidungen** mit Marketing und möglicherweise der Agentur **zu treffen**.

Je nach technischem Stand der vorhandenen E-Mail-Infrastruktur kann bei einer Implementierung von *BIMI*, die Bereitstellung des Markenlogos in einer geeigneten, digitalen Form sich als deutlich größere Herausforderung herausstellen. Ich gehe daher im Folgenden etwas näher darauf ein.

Angepaßtes Design

Im Fokus von *BIMI* steht die Darstellung des Markenlogos links vor den die jeweilige E-Mail beschreibenden Angaben, wie Absender und Betreff (siehe Abbildung 1). Ungeachtet der vom Benutzer individuell angepassten Schriftgröße ist somit von einer quadratischen Darstellung mit einer Kantenlänge rund um die 10 mm auszugehen.

Abbildung 2: Größen- und Detailwahl

Bei nicht schon quadratisch geformten Logos wird die Darstellung innerhalb der verfügbaren Kantenlänge so weit verkleinert, dass die längste Seite passt. Je nach Ausgangsform und Komplexität, gehen in der stark verkleinerten Darstellungsform möglicherweise nicht bloß nur Details "*unter*", sondern beeinflussen auch die Wiedererkennung des Markenlogos.

> Es macht unter Umständen daher Sinn, sich vorab mit Themen wie *Monogramm-Logo* (z.B. die Reduktion auf das "*N*" von *Netflix*), *Brand Icon* (z.B. der angebissene Apfel von *Apple*) oder gar *Brand Abbreviation* (z.B. das "*T*" als Kurzform für *Deutsche Telekom*) auseinander zu setzen.

Abbildung 3: Darstellungsformen

Zusätzlich gibt es drei Varianten, in denen das eigene Logo dargestellt werden könnte:

- Kreis (*circle*)
- Abgerundet (*rounded rectangle*)
- Quadrat (*square*)

Während die Variante "*Quadrat*" alle vorhandenen Bildinformationen des Markenlogos wieder gibt, werden in den anderen Varianten die Ränder einfach abgeschnitten. Dies sollte bei der Größen- und Detailwahl zusätzlich beachtet werden (siehe linkes Bild in Abbildung 2).

In welcher Variante die Darstellung letztendlich erfolgt, wird durch den E-Mail-Client festgelegt. Entweder hat sich der Hersteller für eine Variante fest entschieden oder er überlässt dem Anwender

die Wahl. Einen direkten Einfluss seitens des Markeninhabers, in welcher Variante sein Logo dargestellt werden soll, gibt es aber nicht.

Abbildung 4: Resistente Form

Lässt man jedoch entsprechend Abstände zu den Rändern und den Hintergrund transparent, wird das Markenlogo zusätzlich zu der bereits oben erwähnten Thematik, hinsichtlich der zu erwartenden Kantenlänge der physikalischen Darstellung, nochmals kleiner, aber dafür wird es in jeder Variante einheitlich dargestellt.

Vektorbasierte Grafik

Ungeachtet der zu treffenden Entscheidungen hinsichtlich möglicher Designanpassungen, darf das Markenlogo nicht als pixelbasiertes Raster-Bild (*PNG*, *JPEG* oder *TIFF*), sondern als vektorbasierte Grafik im Format *Scalable Vector Graphics (SVG)* vorliegen. Wie der Name des Formates schon vermuten lässt, können hierbei Grafiken beliebig in ihrer Größe skaliert werden, ohne das Kanten oder Details verwaschen und körnig dargestellt werden. Generell wird im Rahmen der Entwicklung und Verwendung von "*Responsive Designs*" die Verwendung von besser skalierbaren *SVG*-Grafiken forciert, um auch genügend Bildinformationen für hochauflösende Displays bereitstellen zu können.[17]

Der weitere Vorteil das sich die Dateigröße von Bildern trotz steigender Auflösung hinsichtlich ihrer Darstellung nicht verändert, scheint bezogen auf die mehrfach schon angesprochene, zu erwartende, geringe physikalische Darstellungsgröße nicht unmittelbar als erforderlich zu wirken, allerdings wurde die Dateigröße für Markenlogos innerhalb der *BIMI*-Spezifikation auf 32 Kilobytes (dies entspricht etwa 16 Schreibmaschinenseiten) begrenzt.

SVG ist eine Skriptsprache zur Beschreibung zweidimensionaler Vektorgrafiken basierend auf *XML* (*Extensible Markup Language*). Die erste Spezifikation wurde von der W3C im Jahr 2001 veröffentlicht[18].

[17] *Anmerkung: Auch für "Favicons" wird mittlerweile das SVG-Format verwendet, so dass hier das Markenlogo möglicherweise unverändert wiederverwendet werden kann.*
[18] "*Scalable Vector Graphics (SVG) 1.0 Specification*" (W3C, 04.09.2001)

Zur Veranschaulichung dieses Formats ein einfaches Bild mit zwei Elementen einmal in seiner gerenderten Form und einmal als beschreibendes Skript:

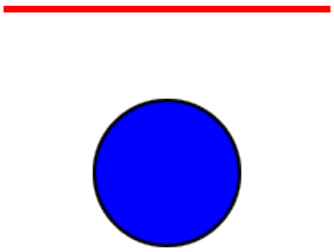

Abbildung 5: Einfaches Beispiel

```svg
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<svg xmlns="http://www.w3.org/2000/svg"
     version="1.2"
     baseProfile="tiny-ps"
     width="200"
     height="200"
     viewBox="0 0 200 200">
  <!-- Eine einfache rote Linie -->
  <line
     x1="10"
     y1="10"
     x2="190"
     y2="10"
     stroke="red"
     stroke-width="4"
     id="line1" />
  <!-- Ein blauer Kreis -->
  <circle
     cx="100"
     cy="100"
     r="40"
     fill="blue"
     stroke="black"
     stroke-width="2"
     id="circle1" />
</svg>
```

Die in dem Skript verwendeten Zahlen sind nicht fixe Position auf einem Raster, sondern als relative Angabe zu dem mittels **`width`**, **`height`** und **`viewBox`** definiertem Dokument zu verstehen. Mit **`line`** und **`circle`** werden die beiden im Bild enthaltenen Elemente beschrieben.

> Wenn man das Markenlogo bisher nur als pixelbasiertes Raster-Bild vorliegen hat, ist eine Konvertierung in das *SVG*-Format auch mit teurer, KI-gestützter Software **nur bedingt möglich** und daher die vektorbasierte, erneute qualitative Erstellung durch einen **humanen Grafiker** zu bevorzugen. Mir bekannte "*Ergebnisse*" KI-gestützter Konvertierungen, wiesen entweder qualitative Einbußen (wie z.B. Risse und Lücken) bei höheren Darstellungsauflösungen auf oder sprengten das Limit von 32 kb.

Die Bilderstellung muss aber nicht per Texteditor erfolgen, sondern kann über ein vektorbasiertes Grafikprogramm stattfinden. Statt das Ergebnis der Anwendung der Zeichentools als Bildinformation zu speichern, wird quasi die Anwendung der Tools in ihrer Art und ihrem Umfang als reproduzierbares Script abgelegt. Um eine bildhafte Abbildung zu erhalten, muss dieses Script erst für eine beliebige Auflösung "*gerendert*" werden.

Angepasstes Dateiformat

Liegt das eigene Markenlogo (nun) als vektorbasierte Grafik vor, muss es noch in ein speziell für diese Verwendung angepasstes Format *SVG Tiny Portable/Secure 1.2* (`tiny-ps`)[19] überführt werden. Hierbei handelt es sich um eine von der Spezifikation *SVG Tiny 1.2* (`tiny 1.2`)[20] abgeleiteten Variante, bei der Sicherheit als Portabilität im Vordergrund steht und welche bereits für die schnelle Verarbeitung auf Geräten mit geringer Rechenleistung optimiert wurde.

> Es kommt ein reduzierter Befehlssatz (wie `path`, `rect`, `circle` oder `line`) zum Einsatz und auf eingebetteten Elemente wurde verzichtet. Reine Text-Elemente müssen daher in allgemein auf den Endgeräten verfügbaren Schriften dargestellt werden oder bereits bei der Bilderstellung in Pfade konvertiert werden.

Auch wenn der reduzierte Befehlssatz den Funktionsumfang hinsichtlich beispielsweise Filtereffekte, Animationen oder gar eingebettete Schriften einschränkt, so sind auf der anderen Seite aber *XSS*-Angriffe, *Phising*- oder *Clickjacking*-Versuche durch die fehlende Unterstützung interaktiver Elemente ausgeschlossen.[21] Zudem erlaubt das Format keine komplexen Dateistrukturen mehr,

[19] Entwurf - "*SVG Tiny Portable/Secure*" (Brotman & Adams, 01.05.2025)
[20] "*SVG Tiny 1.2 Specification*" (W3C, 22.12.2008)
[21] "*Understanding SVG Files and the Dangers of XML Exploits*" (Cloudmersive, 05.05.2025)

wodurch das Sicherheitsrisiko beim bloßen Anzeigen oder Laden einer *SVG*-Datei deutlich minimiert wird.[22]

Anders als bei der im vorherigen Kapitel thematisierten Konvertierung existieren hierfür aber zahlreiche Scripts und Online-Tools, welche für meine Zwecke problemlos funktioniert haben - zumindest wenn man schon zuvor auf etwaige funktionale Einschränkungen geachtet hat.

Die *BIMI Group* selbst stellt einerseits ein Skript zur Verfügung, welches den *Adobe Illustrator* befähigt direkt in diesem Format zu speichern, und andererseits einen Konverter für Windows und MacOS.[23] Mit `svgtinyps`[24] steht auch ein Konverter für weitere Plattformen zur Verfügung und online stellen *EasyDMARC*[25], *Convertio*[26] oder *FreeConvert*[27] auch noch Möglichkeiten bereit bestehende *SVG*-Dateien in das `tiny-ps`-Format umzuwandeln.

Analog zu dem *SVG*-Beispiel im vorangegangen Kapitel, sollten in der umgewandelten Datei die Angaben **`version="1.2"`** sowie **`baseProfile="tiny-ps"`** enthalten sein und sich das Markenlogo unverändert darstellen lassen.

Zertifikat zur Bestätigung der Echtheit der Marke

Um sich die Verbindung eines bestimmten Markenlogos zu einer entsprechenden Domain von einer *Mark Verifying Authority* (*MVA*), einer akkreditierten Zertifizierungsstelle (ähnlich einer *CA*), beglaubigen zulassen, gibt es grundsätzlich zwei unterschiedliche Zertifikate:

- ***Verified Mark Certificate*** *(VMC)* - für registrierte Marken
- ***Common Mark Certificate*** *(CMC)* - für gebräuchliche Marken

Der wesentliche Unterschied liegt im Verifizierungsniveau[28] und den Anforderungen an die Marke.

Ein *VMC*-Zertifikat ist der aktuelle, international anerkannte Standard, der von zertifizierten Ausstellern[^vmc-issuers] herausgegeben wird. Ähnlich wie bei *EV-SSL*-Zertifikaten (*Extended Validation Certificate*)[29] ist eine strenge Identitätsprüfung des Unternehmens erforderlich, bei der Handelsregisterauszüge oder andere Unternehmensdokumente (z.B. Handelsregisternummer, Gründungsurkunde) von der akkreditierten Zertifizierungsstelle überprüft werden. Zusätzlich muss für

[22] *"Hackers are sneaking malware into SVG images to bypass antivirus - here's what we know"* (TechRadar, 08.09.2025)
[23] Github - `authindicators/svg-ps-converters`
[24] Github - `SRWieZ/svgtinyps-cli`
[25] EasyDMARC - *"BIMI Logo Converter"*
[26] Convertio - SVG-zu-PS
[27] FreeConverter - SVG-zu-PS
[28] "*Minimum Security Requirements for Issuance of Mark Certificates*"
[29] Wikipedia - *"Extended-Validation-Zertifikat"*

das jeweilige Markenlogo eine registrierte Markenanmeldung beispielsweise innerhalb Deutschlands[30], der EU[31] oder den USA[32] vorliegen.

Für viele international tätige Unternehmen ist eine Markenanmeldung auf europäischer Ebene besonders attraktiv, da sie in allen 27 EU-Staaten gilt und bereits ab *850€* zu bekommen ist. Für eine Anmeldung am *Deutschen Patent- und Markenamt* würden alleine schon um die *300€* fällig werden.

Dadurch wird die Entscheidung, ob es sich bei dem Logo um eine legitime Marke handelt zwar ausgelagert, aber auf der jeweiligen Ebene einheitlich getroffen. Die Gefahr von nachgemachten Marken und der damit verbundenen Irreführung von E-Mail-Empfängern wird so erheblich reduziert.

Mit *Common Mark Certificate (CMC)*[33] steht eine vereinfachte Variante zur Verfügung, welche keine offizielle Markenregistrierung voraussetzt. Eine *BIMI*-Implementierung mit einem *CMC*-Zertifikat ist schneller möglich, da die Anforderungen hinsichtlich eines Nachweises von Markenrechten weniger streng sind. Hier reicht es aus, wenn man eine öffentliche Verwendung des Logos über mindestens 12 Monate nachweisen kann und es somit als "*gebräuchlich*" gilt. Durch dieses geringere Verifizierungsniveau können zeitgleich Zertifikate für sehr ähnlich aussehende Logos, aber für ganz andere Domains mit abweichenden Inhabern ausgestellt werden.

Für über Pilotprojekte oder interne Tests hinausgehende Implementierungen sollte auf die Verwendung von *CMC*-Zertifikaten allerdings verzichtet werden. *Apple Mail* erkennt keine *CMC*-Zertifikate an und *Google Mail* stellt beim einem *CMC*-Zertifikat zwar das entsprechende Markenlogo da[34], verzichtet aber auf den bei *VMC*-Zertifikaten üblichen blauen "*Verifiziert*"-Haken.[35]

Als grobe Preisindikation würde ich an dieser Stelle ohen Gewähr etwa *1000€* bis *1400€* pro Jahr für ein *VMC*-Zertifikat angeben. Das Hosting des Zertifikates sowie dem dazugehörigen, verifiziertem Markenlogo ist stellenweise inklusive. Hierdurch könnte sich der administrative Aufwand bei "*Verlängerungen*" bzw. erneute Ausstellungen erheblich vereinfachen.

Zwar sind vereinzelt Preisnachlässe für *CMC*- gegenüber den *VMC*-Zertifikaten festzustellen, aber mit gerade mal *10-15%* verbleiben immer noch Preise, die auch für erste Schritte wirtschaftlich weiterhin gegen sie sprechen.

Yahoo und *Fastmail* unterstützen aktuell auch *BIMI*-Implementierung mit selbst-signierten Zertifikaten.[36] Entsprechendes Knowledge mit Zertifikaten vorausgesetzt, liessen sich so erste Erfahrungen sammeln. Aufgrund der geringen Anteile auf deutschen E-Mail-Provider-Marktes (< *10%*)

[30] Deutsches Patent- und Markenamt (DPMA)
[31] European Union Intellectual Property Office (EUIPO)
[32] United States Patent and Trademark Office (USPTO)
[33] *"Announcing Common Mark Certificates"* (BIMI Group, 26.09.2024)
[34] *"Google announces support for CMCs with BIMI"* (Spam Resource, 24.09.2024)
[35] *"VMC vs CMC: Understanding the New Trust Certificates for Brands"* (Bimimi.io, 13.10.2025)
[36] *"What email providers support BIMI without a VMC, and what are key considerations for BIMI implementation?"* (Suped, 03.06.2025)

ergibt sich hierdurch allerdings keine ernstzunehmende, kostengünstige Alternative zu einem (echten) *BIMI* mit *VMC*-Zertifikat.

Technische Implementierung

Der "*Request for Comments* (RFC)" für *BIMI* befindet sich aktuell noch in Bearbeitung[37], liegt aber in einer schon lesbaren, über 30 Seiten starken Fassung vor. Die eigentliche, technische Implementierung von *BIMI* für E-Mail-Versender ist, wenn alle obenstehenden Voraussetzungen erfüllt sind, jedoch auch ohne vorheriges Lesen des Dokumentes schnell gemacht.

Dazu muss das entsprechende Markenlogo und gegebenenfalls das öffentliche Zertifikat über beliebige Webserver publiziert werden.Abgesehen davon, dass diese das Schema "*HTTPS*" unterstützen müssen, gibt es keine weiteren Anforderungen seitens *BIMI*. Diese können also auch einer anderen Domain als der des noch zu setzendem *BIMI*-Eintrages angehören.

Bei einigen *BIMI*-Umsetzungen bekannter Marken, liegen das Markenlogo als auch das *VMC*-Zertifikat auf einem Webserver des Ausstellers. Dadurch wird die Implementierung und wahrscheinlich auch der Austausch des Zertifikates nach Ablauf erheblich vereinfacht.

Der Aufbau des für *BIMI* erforderlichen Eintrages im *DNS* ähnelt doch sehr den Einträgen für *DKIM* oder *DMARC*.

```
default._bimi.mjniessen.com. IN TXT "v=BIMI1;
↪  l=https://mjniessen.de/images/mj-bimi.svg; a="
```

Auch hier wird ein sprechendes Schlüsselwort, in dem Falle "*bimi*", mit einem Unterstrich davor erwartet. Auf diese Weise kommt der Eintrag nicht mit einer möglicherweise schon bestehenden Subdomain oder gar einem künftigen Host mit gleichem Namen in die Quere.

Ähnlich wie bei *DKIM* wird kann zusätzlich noch ein **`selector`**, in diesem Falle ein "*BIMI-Selector*", verwendet werden, um gegebenenfalls den E-Mail-Clients mitzuteilen selektiv auf andere *BIMI*-Einträge zuzugreifen. Dies könnte bei einer Kampagne zur temporären oder zur generellen Änderung des Markenlogos hilfreich sein. In diesem Fall müsste jeder ausgehenden E-Mail der entsprechende "*BIMI-Selector*" (**`s=`**) mittels der folgenden Zeile im E-Mail-Header beigegeben werden:

```
BIMI-Selector: v=BIMI1; s=newselector
```

FÜr den Anfang sollte jedoch der **`default`**-Selektor erstmal reichen. Dieser wird nach Spezifikation von den unterstützenden E-Mail-Clients genutzt, wenn kein oder gar ein fehlerhafter "*BIMI-Selector*"

[37] "*Brand Indicators for Message Identification (BIMI)*" (09.10.2025)

in der E-Mail vorhanden ist. Auf diese Weise bleibt der E-Mail-Header unverändert, was die Implementierung vereinfacht.

Für die entsprechende Domain, hier **`mjniessen.com`**, wird also ein **`TXT`**-Eintrag unter **`default._bimi`** erwartet. Wie schon fast üblich, beginnt dieser mit der Angabe der Version (**`v=`**) der dahinter verwendeten Spezifikation. In unserem Fall handelt sich hier um die Version **`1`** von **`BIMI`**, daher darf die Zahl hinter dem **`I`** auch nicht fehlen. Ich empfehle stets die Schreibweise aus der jeweiligen *RFC* zu verwenden, welche in diesem Fall ausschliesslich die Version in Grossbuchstaben angibt.

Die *URL* des zuvor abgelegten Markenlogos wird als **`location`** mit dem Parameter **`l=`** angegeben. Dahinter folgt die *BIMI Assertion* (**`a=`**), also die *URL* des vom *MVA* ausgestellten Zertifikates zur bescheinigt der Echtheit der Marke. Die Angaben werden jeweils mit einem **`;`** voneinander getrennt. Auch wenn mir das Leerzeichen optional erscheint, verbessert es die Lesbarkeit und wird ebenfalls in der Spezifikation verwendet.

Das Zertifikat enthält ebenfalls das Markenlogo, in dem Fall ist die Angabe über die **`location`** zu der nicht zertifizierten Version der Markenlogos als redundant oder Fallback zu betrachten. Dennoch sollte aber hier, die exakt selbe *SVG*-Datei verwendet werden, die auch bei dem Prozess der Zertifikatserwerbung verwendet wurde.

Im Falle von **`mjniessen.com`** und somit des obenstehenden Beispiels, bleibt die Angabe des **`authenticator`** mit **`a=`** leer, da das verwendete Logo weder die Voraussetzungen für ein *VMC*- noch für ein *CMC*-Zertifikat erfüllt und mir daher noch keiner der genannten Aussteller ein derartiges Zertifikat ausstellen wollte.

Es wird somit bei den E-Mail-Clients der treibenden Kräfte von *BIMI* nicht angezeigt, was ich aber als durchaus positiv werte, da es sonst ausreichend Raum für entsprechenden Missbrauch geben würde und somit *BIMI* seine Wirkung verfehlen würde.

Erklärung

Dieses Dokument wurde von mir, Maurice-Jörg Nießen, nach bestem Wissen und Gewissen erstellt. Es erhebt weder einen Anspruch auf Vollständigkeit, noch stellt es eine rechtliche Beratung dar. Die Nutzung der enthaltenen Informationen erfolgt auf eigenes Risiko. Für etwaige Schäden, die aus der Verwendung dieses Dokumentes resultieren, wird keine Haftung übernommen.

Jegliche Weitergabe oder Veröffentlichung dieses Dokuments – auch auszugsweise – bedarf der vorherigen schriftlichen Zustimmung des Autors.

Maurice-Jörg Nießen