

Technisches Setup

Service-Beschreibung

imc Learning Suite

10. Oktober 2023

Vorwort und Zielsetzung

Dieses Dokument beschreibt die Serviceleistungen, die das imc Projektteam im Rahmen des **Technischen Setups** (Technical Setup) eines Implementierungsprojekts des Learning Management System (LMS) imc Learning Suite erbringt. Das Technische Setup umfasst verschiedene technische und organisatorische Leistungen, die zur Installation und zum technischen Betrieb der Software – sowohl in der Cloud als auch bei on-premise Installationen – nötig sind.

Das Technische Setup umfasst (a) eine technisch funktionsfähige **Installation des Standardprodukts**, (b) das **Codeline-Management und Lizenz-Management** inklusive der generellen Einrichtung der Sprachpakete, (c) die **technische Integration für URL und Mailversand**, und (d) die **Umsetzung des Design-Pakets**, d.h. die Anpassung des User Interfaces an das CI/CD (Corporate Design).

Aus diesem Grund beinhaltet die Service-Beschreibung die enthaltenen Arbeitspakete unter Betrachtung der folgenden Aspekte:

- **Beschreibung der zu erbringenden Leistungen**, die im Rahmen des technischen Setups durch das imc Projektteam erbracht werden. Das Dokument beschreibt auch zusätzliche Optionen, die ggf. als Zusatzleistungen im Rahmen des Scopes des Implementierungsprojekts erbracht werden können.
- **Beschreibung der Zuständigkeiten und Verantwortlichkeiten**, die zum Teil auf Seiten imc und zum anderen Teil auf Seiten des Kunden liegen.
- **Beschreibung des Vorgehens, des Ablaufs und zeitlicher Abhängigkeiten** für das technische Setup, damit für alle Beteiligten ein transparenter Blick auf die einzelnen Schritte möglich ist.

Installation des Standardprodukts

Dieser Abschnitt beschreibt die Installation des Standardprodukts der imc Learning Suite im Rahmen des Technischen Setups. Grundsätzlich gilt es bei der Installation der Systeme zwischen Cloud- und on-premise-Betriebsmodell zu unterscheiden.

- Bei einem **Cloud-Betriebsmodell** übernimmt die imc die Installation der Systeme (sowohl Produktivsystem als auch weitere Umgebungen sofern beauftragt) und der Kunde ist hierzu nicht involviert.
- Im **on-premise-Betriebsmodell** führt die imc die Installation der Systeme zusammen mit dem Kunden durch. Dies umfasst jedoch nur eine Umgebung, i.d.R. die Produktivumgebung. Weitere Umgebungen müssen vom Kunden selbst installiert werden, es sei denn, es liegt eine gesonderte Vereinbarung vor, dass imc auch bei der Installation weiterer Umgebungen unterstützt. Im on-premise Betriebsmodell stellt die imc die entsprechenden Installationspakete dem Kunden zur Verfügung. Die eigentliche Installation wird dann von imc durchgeführt, wobei der Kunde bei dieser Installation anwesend sein sollte, da im Anschluss die Verantwortung für die Umgebung an den Kunden übergeht. Werden im Zuge der Installation Konfigurationsdateien (die für den technischen Betrieb benötigt werden) angepasst, so sind diese an imc zu übermitteln, damit Sie in den zukünftigen Auslieferungen beinhaltet sind. Gleiches gilt für den Fall, dass der Kunde neben einer Produktivumgebung weitere Umgebungen betreibt (Test, Stage, Dev etc.). Auch in diesem Fall muss dies imc mitgeteilt werden, damit zukünftige Auslieferungen dies berücksichtigen können. Werden im Verlauf des Projektes weitere Auslieferungen dem Kunden zur Verfügung gestellt, so werden diese Aktualisierung durch den Kunden selbst durchgeführt.

Im Zusammenhang mit der Installation des LMS im on-premise-Betriebsmodell wird an dieser Stelle auf die offiziellen Dokumente der Software bzgl. Systemvoraussetzungen und Installationshinweise verwiesen. Der Kunde ist verpflichtet, die notwendigen Voraussetzungen für eine on-premise Installation zu gewährleisten, bevor ein Techniker der imc die Installation durchführen kann.

Die von einem imc Techniker durchgeführte Installation umfasst folgende Bereiche: (i) Java SDK, (ii) Tomcat Applikationsserver, (iii) imc-Applikationsdateien, (iv) systemspezifische Konfiguration (hierzu zählt auch die Anbindung an den bereitgestellten SMTP-Server). Falls gewünscht, kann auch eine Anbindung der Applikation über ISAPI an einen IIS-Webserver erfolgen, um etwa Windows-SSO zu ermöglichen. Darüberhinausgehende Anbindungen und Konfigurationen, wie etwa die Anbindung von Reverse-Proxy, WAF o.Ä. sind nicht Teil unseres Leistungsspektrums.

Hinweis: Jede Umgebung (z.B. Produktion oder Test oder Stage) hat in den technischen Betriebsparametern die Information hinterlegt, um welche Umgebung es sich handelt (**System-Kontext**). Dies erlaubt, zwischen produktiven und nicht produktiven Umgebungen zu unterscheiden (z.B. versenden nur produktive Umgebungen Mails, während nicht produktive Umgebungen Mails immer im Testmodus versenden) bzw. umgebungsspezifische Konfigurationen zu erlauben (im Bereich URLs, SSO etc.). Im Zuge des Abschlusses des Implementierungsprojekts empfehlen wir – sofern mehr als die Produktivumgebung genutzt werden – die Datenspiegelung von

Produktion auf die weiteren Umgebungen zu testen, damit gewährleistet ist, dass die entsprechenden Einstellungen vollständig übernommen werden (z.B. der SSO auf der Testumgebung).

Unabhängig vom Betriebsmodell existiert für jeden Kunden ein **imc internes Referenzsystem**, welches für die Vorbereitung von Auslieferungen sowie das Nachstellen von Problemen oder die Implementierung von kundenspezifischen Anpassungen (wenn im Betriebsmodell möglich) genutzt wird. Auf Referenzumgebungen haben Kunden keinen Zugriff.

Nach Auftragseingang und Initialisierung des Projekts durch den imc Projektmanager wird die Installation der Systeme auf imc Seite eingeplant und vorgenommen (im Cloud-Modell) bzw. mit dem Kunden koordiniert (falls on-premise-Modell). Der imc Projektmanager involviert hierzu die technische Abteilung der imc und koordiniert Bereitstellung der für die Erstinstallation notwendigen Pakete. Die Verfügbarkeit des Systems bzw. der Installationspakete benötigt in der Regel eine Vorlaufzeit von zirka zwei Wochen.

Hinweis: Im Cloud-Betrieb hat das Projektteam Zugriff auf die Umgebungen. Für on-premise Installationen muss der Zugriff für das imc Projektteam (und auch später den imc Support) auf die Web-Applikation frühzeitig geklärt werden.

Codeline Management & Lizenz-Management

Die imc verwaltet für jeden Kunden den aktuellen Auslieferungsstand der Software. Hierzu werden die Kundensysteme im imc **Codeline-Management-System** hinterlegt und verwaltet. Es gibt grundsätzlich drei verschiedene Arten von Codelines:

- Dedizierte Codeline (Cloud-Betriebsmodell)
- Dedizierte Codeline (on-premise-Betriebsmodell)
- Cloud-Codeline (keine dedizierte Codeline)

Eine dedizierte Codeline (Cloud oder on-premise) ermöglicht es grundsätzlich kundenspezifische Anpassungen für Kunden zu implementieren, sofern es einen Codebereich umfasst, der Anpassungen am Sourcecode erlaubt. In der Cloud-Codeline gibt es grundsätzlich keine Möglichkeit kundenspezifische Anpassungen am vorhandenen Sourcecode zu implementieren.

Die Art der Codeline steht bei Beauftragung bereits fest, sodass das imc Projektteam im Rahmen des technischen Setups die nötigen Informationen an die entsprechende Abteilung weiterleitet.

Hinweis: Sofern eine dedizierte Codeline verwendet wird, erfolgt im Rahmen des Projekts eine regelmäßige Aktualisierung der Codeline mit Patches und Innovationspaketen durch das imc Projektteam. Ebenso die zeitnahe und regelmäßige Aktualisierung der Umgebung mit aktuellen Softwareversionen des LMS ist notwendig und obliegt entweder in der Verantwortung des Projektteams (Cloud-Betrieb) oder des Kunden / der Kunden-IT (on-premise-Betrieb). Im Falle der Cloud-Codeline finden die Softwareaktualisierung automatisiert statt, so dass die Umgebungen immer auf dem neuesten Softwarestand sind.

Im Rahmen des **Lizenz-Managements** werden durch das imc Projektteam alle beauftragten Module sowie Sprachpakete lizenziert. Das imc Projektteam übernimmt hierbei die Beantragung der notwendigen Lizenzen sowie die Konfiguration der Sprachpakete.

Die Lizenz- und Sprachpakete sind in aller Regel bereits aus der Beauftragung heraus klar, sodass das imc Projektteam diese nach erfolgreicher Installation des Systems konfiguriert. Die wichtigsten Aspekte sind hierbei die Nutzerzahl, die verwendeten Plattformsprachen sowie die zusätzlichen Module, die explizit lizenziert werden müssen.

Stehen dem Kunden mehrere Umgebungen zur Verfügung, so wird grundsätzlich nur eine Lizenz verwendet. Die aktivierte Lizenz ist Teil der Datenbank und wird im Zuge einer Datenspiegelung von Produktion auf nachgelagerte Systeme automatisch übernommen. Die Lizenz kann aber auch manuell auf jeder Umgebung eingespielt werden.

Technische Integrationen

Im Rahmen des technischen Setups erfolgt auch die Einrichtung der URL (inklusive sicheren Zugriff) und des Mailversands.

Koordination URL und SSL-Zertifikat

Die Technische Koordination hat zum Ziel, dass das LMS vor unter der gewünschten URL erreichbar und durch ein SSL-Zertifikat abgesichert ist. Bis zur Umstellung auf die URL des Kunden ist das LMS im Cloud-Betrieb unter einer temporären URL der imc erreichbar.

Die imc Learning Suite ist eine webbasierte Applikation, welche über einen Browser (bspw. Google Chrome, Firefox, Edge) geöffnet wird. Damit das LMS unter der vom Kunden gewünschten URL erreichbar ist, benötigt imc gewisse Informationen. Für die produktive Nutzung der Learning Suite, sollte die Anwendung auf einer durch den Kunden registrierten Domain (Internet-Adresse) und einem für diese Domain passenden SSL-Zertifikat laufen. Die Adressierung der Website wird dann dementsprechend über eine vom Kunden definierte URL abgeschlossen.

Hinweis: Es besteht auch die Möglichkeit, den Betrieb des LMS in der Cloud komplett über eine URL von imc abzubilden. Hierzu bietet imc Sub-Domains an (in Abhängigkeit des Cloud-Betriebsmodells).

Wichtiger Hinweis: Bei mehreren Systemen (Produktivumgebung, Testumgebung) werden alle URLs und die jeweiligen SSL-Zertifikate benötigt (bestenfalls liegen diese Informationen bereits bei Projektstart vor). **Die Verantwortlichkeit liegt hier beim Kunden die erforderlichen Schritte einzuleiten und die Informationen und Dateien imc bereitzustellen.** Das imc Projektteam kann hier beratend unterstützen bzw. aktiv durch die Erstellung eines Zertifikatrequests (CSR) zur einfacheren Beantragung eines SSL-Zertifikats durch den Kunden.

Im Cloud-Betrieb leitet der imc Projektmanager nach Erhalt der URL und des SSL-Zertifikats diese an das imc Hosting weiter. Nachdem alle Vorbereitungen vom imc Hosting abgeschlossen wurden, kann die finale Umstellung der URL vorgenommen werden.

Das Ziel der URL-Umstellung ist es, dass die vom Kunden registrierte Internet-Adresse (Domain), auf den LMS-Server verweist, so dass ein Nutzer bei einem Aufruf der URL auf das LMS gelangt. Dazu muss der Kunde eine Weiterleitung (DNS-Eintrag) bei sich einrichten. Die Empfehlung der imc ist es hier einen CNAME Eintrag zu setzen, wobei alternativ auch ein A Record möglich ist. Je nach Entscheidung des Kunden stellt das imc Projektteam dem Kunden die jeweils benötigten Informationen für den DNS-Eintrag zur Verfügung (URL imc Trafficmanager oder IP-Adresse). Sobald der DNS-Eintrag vom Kunden gesetzt wurde, kann das imc Hosting die finale Umstellung auf imc Seite vornehmen und das imc Projektteam informiert den Kunden, sobald das System unter der gewünschten URL erreichbar ist.

Im Folgenden werden zusätzliche detailliertere Informationen zu diesem Thema erläutert:

Ein SSL-Zertifikat dient als verbindlicher Identitätsnachweis – darüber hinaus sind in dem Zertifikat Informationen enthalten, mit dem Browser und Server eine Verschlüsselung aufbauen können. Dadurch ist die Kommunikation vom Computer, Smartphone oder Tablet zu der Website (dem LMS) abgesichert und verschlüsselt.

Für die produktive Nutzung des LMS, muss die Anwendung auf einer durch den Kunden registrierten Domain und einem für diese Domain passenden SSL-Zertifikat laufen. Die betrifft alle Betriebsmodelle (Cloud und on-premise). Grundsätzlich kann eine eigene Domain oder eine Sub-Domain (z.B. <https://lms.customer.com> oder <https://academy.customer.com>) einer bestehenden Domain verwendet werden. Die Nutzung eines Kontextpfades (z.B. <https://customer.com/academy> oder <https://customer.com/lms>) einer bestehenden Domain ist nicht möglich.

Von Seiten imc wird die Verwendung einer Subdomain empfohlen. Ein großer Vorteil bei der Verwendung einer Subdomain besteht darin, dass es für die IT des Kunden oftmals einfacher ist ein Zertifikat für die Subdomain zu erlangen, da bereits eine Registrierung für die Hauptdomain erfolgte. Sofern für das LMS keine Subdomain verwendet werden soll, ist es auch möglich eine neue Domain zu registrieren. In diesem Fall muss dies durch den Kunden selbst erfolgen – die imc wird keine Domains erwerben.

Im Falle, dass das LMS in der Cloud durch imc betrieben wird, erfolgt die Bereitstellung des SSL-Zertifikats für eine Domain oder Sub-Domain an die imc auf folgende Art:

- Entweder als eine Datei in .pfx Format (Zertifikate inklusive Private Key) + Passwort
- Oder als einzelne Dateien:
 - o Zertifikat in .crt, .cer, .cert, .pem Format
 - o Private Key in .key Format + Passwort
 - o Zwischenzertifikate

Wichtig ist, dass die **Zwischenzertifikate (Intermediates)** mitgeliefert werden. Zwar kann die sichere Verbindung zur Website aufgebaut werden, aber das Zertifikat wird nicht in allen Webbrowsern als vertrauenswürdig eingestuft wird.

Hinweis: Aus sicherheitstechnischen Gründen ist es wichtig, dass das SSL-Zertifikat und der zugehörige Private Key getrennt der imc zur Verfügung gestellt werden. Es empfiehlt sich getrennte Kommunikationskanäle etc. zu nutzen.

Falls bei der Erstellung eines sogenannten Zertifikatrequests (CSR) Unterstützung benötigt wird, so kann die imc hierbei unterstützen. Ein CSR ist eine Datei, die alle notwendigen Daten und Details beinhaltet (Kontaktdaten & öffentlichen Schlüssel). Damit imc ein CSR erstellen kann, werden nachfolgende Informationen benötigt:

- **Common name:** z.B. lms.customer.com
- **Organisation:** z.B. Customer Name
- **Organisational Unit:** z.B. IT
- **City/ Locality:** z.B. Munich
- **State/ Province:** z.B. Bavaria
- **Country:** z.B. Germany

Mit den vom Kunden bereitgestellten Daten erstellt die imc einen CSR und stellt diesen dann zur Verfügung. Dieser CSR kann dann bei einer Zertifizierungsstelle (CA) registriert werden, um ein SSL-Zertifikat anzufordern.

Hinweis: SSL-Zertifikate verfügen über eine begrenzte Gültigkeitsdauer und müssen regelmäßig aktualisiert werden. Sollte das SSL-Zertifikat abgelaufen sein, so kann die Nutzung des LMS für die Nutzer stark eingeschränkt sein. Im Betrieb des LMS wird der imc Support im Regelfall über den baldigen Ablauf eines Zertifikats informieren. Die Verantwortung für die Bereitstellung eines aktualisierten Zertifikats liegt jedoch auf Kundenseite. Daher sollte der Kunde selbst die Erneuerung von Zertifikaten im Auge behalten.

Wichtiger Hinweis: Im on-premise Betriebsmodell ist die IT des Kunden für die Bereitstellung und Aktualisierung eines gültigen SSL-Zertifikats zuständig. Von Seiten imc kann hier nicht bei der Erstellung unterstützt werden. Das SSL-Zertifikat muss zum Zeitpunkt der Erstinstallation bereitgestellt werden, da es sonst zu technischen Problemen und Zusatzaufwand im Verlauf des Projekts kommen kann.

Sobald die imc die relevanten Dateien des SSL-Zertifikats zur Verfügung gestellt bekommen hat, kann die Umstellung der Domain erfolgen. Ziel der Umstellung ist es, dass die Internet-Adresse (Domain) auf den LMS-Server verweist, so dass ein Nutzer bei einem Aufruf der URL auf das LMS gelangt. Hierzu muss von Kundenseite eine Weiterleitung (DNS-Eintrag) eingerichtet werden.

Im Falle des on-premise-Betriebsmodells obliegt die komplette Einrichtung der IT des Kunden, die den Betrieb des LMS verantwortet. Im Falle des Cloud-Betriebs ergeben sich zwei Optionen:

- **Variante 1: CNAME (empfohlen von imc):** Ein CNAME ist eine Verweisung von Hostname zu Hostname. Im Gegensatz zur zweiten Variante ist diese Art der Weiterleitung flexibler. Zudem ist gewährleistet, auch dynamische IP-Adressen als Ziel ansprechen zu können. Dazu muss folgendes eingerichtet werden:

Einrichtung eines DNS-Eintrag (CNAME) auf den Trafficmanager des LMS

- **Variante 2: A RECORD (nicht empfohlen von imc):** Hier wird eine fixe Weiterleitung auf die IP Adresse Ihres LMS-Servers eingerichtet. Es kann u.U. vorkommen, dass diese sich verändert. In solchen Fällen müsste die Kunden-IT den DNS-Eintrag auf die neue IP-Adresse anpassen und es kann zu Einschränkungen des Zugriffs kommen, die außerhalb der Zuständigkeit der imc liegen. Dazu muss folgendes eingerichtet werden:

Einrichtung eines DNS-Eintrag (A Record) auf die IP-Adresse des LMS-Servers

Hinweis: Die Angaben zum Trafficmanager bzw. die IP-Adresse des LMS-Servers im Cloud-Betrieb werden dem Kunden im Zuge des Technischen Setups mitgeteilt.

Sobald die Weiterleitung (DNS-Eintrag) eingerichtet wurde, erfolgt der letzte Schritt seitens imc Hosting und das imc Projektteam informiert den Kunden, sobald das LMS über die gewünschte Internet-Adresse (URL) erreichbar ist.

Wichtiger Hinweis: Wir raten davon ab, den DNS-Eintrag mit einer externen WAF oder Ähnlichem zu nutzen, da dies zu Supportfällen und unvorhersehbaren Problemen führen kann. Der

Analyseaufwand für solche Supportfälle, bei denen der DNS-Eintrag nicht wie in Variante 1 empfohlen gesetzt wurde, wird die imc gesondert in Rechnung stellen.

Ergänzender Hinweis: Im Standardfall (sofern nicht anders beauftragt) geht das Technische Setup davon aus, dass das LMS unter einer einzigen URL verfügbar sein soll. Grundsätzlich ist es möglich, das LMS unter mehreren URLs zur Verfügung zu stellen (Mandanten mit eigener URL). Eine Nutzung mehrere URLs kann z.B. in einem Szenario mit verschiedenen Zielgruppen sinnvoll sein. Sollte dies Gegenstand der Beauftragung und des gewünschten Szenarios sein, so kann dies durch das imc Projektteam entsprechend koordiniert werden.

Koordination Mailversand

Im Rahmen der Einrichtung der Mailing-Funktionalität des LMS wird sichergestellt, dass das LMS jegliche E-Mails (System-E-Mails, Buchungs-E-Mails, Benachrichtigungen) mit der vom Kunden definierten Absenderadresse (Bsp. ims@customer.com) korrekt versendet.

Wichtiger Hinweis: Im on-premise-Betriebsmodell ist die IT des Kunden verantwortlich dafür, einen eigenen Mailserver zur Verfügung zu stellen, für den das LMS die Erlaubnis hat, Mails versenden können. Die Anbindung des Mailservers erfolgt bereits im Rahmen der Erstinstallation der Standardsoftware. Technische Probleme sind durch die IT des Kunden zu analysieren.

Im Cloud-Betrieb ergeben sich drei Optionen, den Mailversand des LMS zu konfigurieren:

- **Variante 1 (Versand über imc Mailserver; empfohlen):** Der Mailversand des LMS erfolgt über eine Absenderadresse des Kunden (z.B. ims@customer.com oder academy@customer.com). Hierzu muss ein SPF-Record für den Mailserver customer.com durch die Kunden-IT gesetzt werden, da ansonsten die Gefahr besteht, dass Mails als Spam identifiziert werden. Ausnahmefall, für den kein SPF-Record benötigt wird, ist, wenn der Mailserver customer.com nur Mails an seine eigenen Nutzer versendet und der Mailversand durch das LMS explizit erlaubt wird.

Hinweis: Zusätzlich zu einem SPF-Record kann der Mailversand mit einer Signierung erfolgen. Eine DKIM-Signierung wird durch imc unterstützt und kann im Rahmen einer zusätzlichen Beauftragung umgesetzt werden. In diesem Fall erstellt die imc die entsprechenden Schlüsselpaare und stellt Sie der Kunden-IT zur Hinterlegung im DNS-Eintrag von customer.com zur Verfügung.

- **Variante B (direkter Versand über Kunden-Mailserver):** Sollte es nicht möglich sein, einen SPF-Record zu setzen oder der explizite Wunsch existieren, nicht über den imc Mailserver zu versenden, so kann auch der Mailserver des Kunden direkt an das LMS angebunden werden. Der Versand der Mails erfolgt weiterhin über eine Absenderadresse des Kunden (z.B. ims@customer.com oder academy@customer.com). Die direkte Anbindung des LMS an den Mailserver des Kunden benötigt im Rahmen des Technischen Setups keine gesonderte Beauftragung, hat aber zur Folge, dass imc deutlich weniger Möglichkeiten bei der Analyse von Mailproblemen hat.
Folgende drei aktuelle Einschränkungen gilt es zu beachten: (i) der Mailserver muss direkt erreichbar sein (eine VPN-Verbindung ist nicht möglich), (ii) die Authentifizierung erfolgt über SMTP-Auth, d.h. imc benötigt die Anmeldedaten eines Nutzers zur Einrichtung, und aktuell wird nur TLS 1.2 unterstützt, und (iii) die weiteren Sicherheitseinstellungen (Security

Policies) des Mailservers des Kunden liegen in der Verantwortung des Kunden (ggf. muss die IP-Adresse des LMS-Servers freigeschaltet werden oder es gibt Einschränkungen beim Weiterversand an die eigentlichen Empfänger).

Hinweis: In dieser Variante ist aus Sicht des LMS der Mailversand dann abgeschlossen, wenn das LMS die Mail an den Mailserver des Kunden übergeben hat, d.h. der Mailversand im LMS als erfolgreich gekennzeichnet oder protokolliert ist. Alle weiteren Analysen und Untersuchungen, für den Fall, dass die Mail nicht beim Empfänger ankommt, liegen in der Verantwortung des Verantwortlichen für den Mailserver des Kunden und somit außerhalb der Verantwortlichkeit der imc.

- **Variante C (Versand über imc-Absenderadresse):** imc bietet in Ausnahmefällen auch an, dass Mails über eine Absenderadresse der imc versendet wird (z.B. customer@lms-saas.com oder customer@imc-learning.com). Auf Seiten imc werden hierzu die relevanten Sicherheitseinstellungen vorgenommen, um einen erfolgreichen Versand zu gewährleisten. Zu beachten ist jedoch, dass der Kunde keinen Zugriff auf das entsprechende Postfach hat, sollten Nutzer auf die versendeten Mails antworten und für den Empfang von systemseitigen Mails wird von Seiten des Kunden trotzdem eine Empfängeradresse benötigt.

Der imc Projektmanager klärt die relevanten Themen direkt zu Beginn des Einführungsprojekts. Insbesondere für Variante 1 ist das Setzen eines SPF-Records wichtig und der imc Projektleiter wird alle relevanten Informationen hierzu bereitstellen, z.B.:

- *Das Sender Policy Framework (SPF) ist ein offener Standard, der ein technisches Verfahren zur Verhinderung der Fälschung von Absenderadressen spezifiziert. Genauer gesagt schützt die aktuelle Version von SPF - SPFv1 oder SPF Classic genannt - die Absenderadresse des Umschlags, die für die Zustellung von Nachrichten verwendet wird.*
- *SPFv1 erlaubt es dem Besitzer einer Domain, seine Richtlinien für den Mailversand festzulegen, z. B. welche Mailserver er für den Mailversand von seiner Domain verwendet. Bei dieser Technologie müssen zwei Seiten zusammenspielen: (1) der Besitzer der Domain veröffentlicht diese Informationen in einem SPF-Eintrag in der DNS-Zone der Domain, und wenn ein anderer Mailserver eine Nachricht empfängt, die behauptet, von dieser Domain zu kommen, dann kann (2) der empfangende Server überprüfen, ob die Nachricht mit der angegebenen Richtlinie der Domain übereinstimmt. Wenn die Nachricht z. B. von einem unbekanntem Server kommt, kann sie als Fälschung betrachtet werden.*

Dieser SPF-Record kann wie folgt aussehen (genauere Informationen werden immer vom imc Projektleiter bereitgestellt):

domain.com IN TXT "v=spf1 a mx include:spf.imc-hosting.com -all"

Wichtiger Hinweis: Das Setzen dieses SPF-Records liegt in der Verantwortlichkeit des Kunden. Sobald der Eintrag auf Kundenseite gesetzt wurde, gibt der Kunde dem imc Projektmanager Bescheid. Die Prüfung des Eintrags wird dann vom imc Hosting Seite vorgenommen und die Einrichtung ist damit abgeschlossen. Ein späteres Entfernen des SPF-Records kann zur Folge haben, dass Mails nicht mehr die Nutzer erreichen.

Ergänzender Hinweis: Im Standardfall geht das Technische Setup davon aus, dass das LMS unter einer einzigen Absenderadresse Mails versendet. Das LMS erlaubt zusätzlich, die Verwendung mehrere Absenderadressen (z.B. unterschiedliche Absenderadressen pro Veranstalter /

Mandant). Dies kann z.B. bei einem Szenario mit internen und externen Nutzern, bei denen das LMS auch unter mehreren URLs verfügbar ist und für beide Zielgruppen auch unterschiedliche Namen verwendet werden, durchaus sinnvoll sein. In diesem Fall müssen Auswirkungen genau bedacht werden und alle oben genannten Einrichtungen müssen pro Absenderadresse sichergestellt werden.

Umsetzung Design

Im Rahmen des Technischen Setups erfolgt auch die **Anpassung des LMS-Designs an das Corporate Design des Kunden**, um sicherzustellen, dass das LMS optisch dem CI / CD (Logos, Farben, Schrift etc.) des Kunden angeglichen ist. Wichtig zu erwähnen ist, dass an dieser Stelle zwischen Design und Konfiguration unterschieden werden muss. U.a. gehören angezeigte Inhalte (z.B. Navigationseinträge in der Hauptnavigation oder im Footer), das Einblenden / Ausblenden von Buttons und Einstellungen (z.B. Katalogfilter oder Texte / Anordnungen auf Beschreibungsseiten) oder das Systemwordings nicht zum Design und können im Rahmen des Implementierungsprojekts angepasst werden.

Sofern nicht anders beauftragt, erfolgt die Erstellung eines kundenspezifischen Designs durch imc, welches den Mandanten des Systems zugewiesen werden kann. Weitere Designs sind möglich und können gesondert beauftragt werden. Die Designumsetzung erfolgt immer für den Browserzugriff auf das LMS sowie für die beiden Mobilien Standard-Apps (iOS, Android).

Ergänzender Hinweis: Das LMS erlaubt es, pro Mandanten ein eigenes Design zu verwenden und zusätzliche Designs können im Rahmen einer gesonderten Beauftragung umgesetzt werden.

Für einen optimalen Ablauf der Anpassung durch das imc Design-Team, stellt der Kunde dem imc Projektmanager eine Beschreibung des gewünschten Designs zur Verfügung. In der Regel sind dies CI / CD Guidelines oder ein Link zur Unternehmenswebsite. Sollte eine nicht lizenzfreie Schriftart gewünscht sein, so müssen die entsprechenden Webfont Dateien ebenfalls an imc übermittelt werden - imc übernimmt nicht den Erwerb solcher Dateien. Sollte es unterschiedliche Grundfarben im CI / CD des Kunden geben, so ist ein Hinweis mit der bevorzugten Grundfarbe notwendig.

Nach gesammeltem Erhalt aller Informationen übergibt der imc Projektmanager den Auftrag an das imc Design Team. **In der Regel wird das Design dann innerhalb von zwei Wochen erstellt und auf dem Projektsystem eingespielt. Nach dem Einspielen des Designs hat der Kunde die Aufgabe / Verantwortung das Design zu prüfen und ein gesammeltes, nachvollziehbares Feedback an die imc zurückzuspielen. Dies sollte innerhalb von 4 Wochen erfolgen.** Nach Klärung des Feedbacks und der Möglichkeiten zwischen dem Kunden und dem Projektmanager kann ggf. eine Überarbeitungsrunde eingeplant werden.

Sollte auf Seiten des Kunden ein besonderer Bedarf bestehen, die Optionen und Möglichkeiten genauer zu untersuchen, so bietet die imc einen sogenannten **User Experience Design Workshop** mit einem Frontend-Designer an. Dieser i.d.R. halbtägige Workshop benötigt – wenn nicht anders vereinbart – eine gesonderte Beauftragung.