GOVERNIKUS
MULTIMESSENGER

Zukunftssichere Multikanalkommunikation

governikus.de

GOVERNIKUS

Zukunftssichere Multikanalkommunikation

Die Digitalisierung ist in der Kommunikation längst angekommen. Bei Bürger:innen sowie Unternehmen steigt die Erwartungshaltung, auch mit Behörden, Justiz und anderen Organisationen elektronisch kommunizieren zu können. „Schnell und unkompliziert“ ist hier das Credo. Gleichzeitig ist es aus Effizienzgründen innerhalb der Organisationen unerlässlich, die elektronische Kommunikation medienbruchfrei in ihre Weiterverarbeitungssysteme zu integrieren.

Die Einführung von eAkten, wie in den eGovernment- und eJustice-Gesetzen verankert, wird nur dann zielführend umgesetzt werden können, wenn es gelingt, die vielfältigen elektronischen Kommunikationspotenziale auszuschöpfen und sowohl strukturierte als auch unstrukturierte Kommunikation einzubinden.

Heterogen – Nationale und internationale Kommunikationskanäle

Elektronische Kommunikation beschränkt sich keineswegs auf nur einen Zustell- bzw. Empfangskanal. Die Landschaft der Kommunikationskanäle verändert sich rasant und wird zunehmend heterogener, wobei die Anforderungen an Integrität und Authentizität elektronischer Nachrichten immer mehr an Bedeutung gewinnen. Neue Kanäle werden in den kommenden Jahren entstehen, ohne dass deshalb zwingend bereits existierende Kanäle wegfallen werden. „One-in-one-out“ ist also nicht zu erwarten.

Durch die eIDAS-Verordnung der Europäischen Union werden zeitnah weitere sog. elektronische Einschreib-Zustelldienste aus anderen europäischen Ländern hinzukommen, die von unserer Verwaltung empfangen, verarbeitet und auch wieder zurückadressiert werden müssen.

MULTIKANAL
Herausforderung unserer Zeit

Die Herausforderungen im Umgang mit elektronischer Kommunikation sind ebenso vielfältig wie die unterschiedlichen Kanäle:

- Empfangs- und Zustellkanäle müssen in die bestehende IT-Landschaft und verschiedenste fachliche Szenarien integriert werden.
- Neue Standards entstehen, die es zu implementieren gilt.
- Hinzu kommt der Umgang mit kryptografisch behandelten Nachrichten, die ver- und entschlüsselt werden müssen.
- Damit einhergehend sind für verschiedene Kanäle die entsprechenden Zertifikate zu verwalten.
- Der Umgang mit Signaturen beschränkt sich nicht nur auf das Anbringen von eigenen Signaturen, es müssen darüber hinaus gemäß eIDAS-Verordnung auch sämtliche europäische Signaturen verifiziert werden können.
- Die Speicherung von erteilten Zugangseröffnungen, Identitäten und Zertifikaten der Kommunikationspartner sowie die transparente und rechtssichere Nachvollziehbarkeit sind weitere Punkte, die es zu beachten gilt.

Egal ob CIO, System- und Fachadministration oder Sachbearbeitende: Ihre Mitarbeiter:innen werden tagtäglich auf unterschiedlichen Ebenen mit diesen und weiteren Herausforderungen konfrontiert. So entstehen – entgegen der eigentlichen Zielsetzung der Digitalisierung – zeit- und kostenintensive Aufwände durch oftmals proprietäre Insellösungen mit Medienbrüchen in den Prozessen.

Virtuelle Poststelle

Um die vielfältigen Kommunikationswege innerhalb der Verwaltung effizient und zukunftssicher bedienen zu können, ist es nicht zielführend, die Zustell- und Empfangskanäle einzeln an die jeweiligen Fachverfahren oder eAkten-Systeme anzubinden. Es empfiehlt sich stattdessen, eine zentrale, virtuelle, elektronische Poststelle zu etablieren. Diese kann sämtliche elektronische Formate annehmen, weiterverarbeiten und in ein gewünschtes Zielsystem weiterleiten, dabei sämtliche kryptografischen und Identitätsprüfungen übernehmen und ggf. die Originalnachrichten direkt an einen Langzeitspeicher zur Beweiswerterhaltung übergeben. Gleichzeitig wird gewährleistet, dass die Zugangseröffnung von Bürger:innen sowie Unternehmen zentral gespeichert wird, so dass Ihre Organisation die elektronische Kommunikation nicht nur empfangen, sondern auf dem gleichen Weg beantworten kann.

DIE LÖSUNG
Governikus MultiMessenger

Um der Herausforderung Multikanalkommunikation zu begegnen, wurde der Governikus MultiMessenger (GMM) entwickelt. Die intelligente Kommunikationsplattform bietet Lösungen für zukünftige Herausforderungen, die durch die stetige Weiter- und Neuentwicklung von digitalen Kanälen in der elektronischen Kommunikation entstehen.

Digitalisierung von Prozessen, Einführung von eAkten sowie die Integration in bestehende IT-Landschaften: Der GMM ermöglicht eine zukunftssichere, übergreifende Multikanalstrategie.

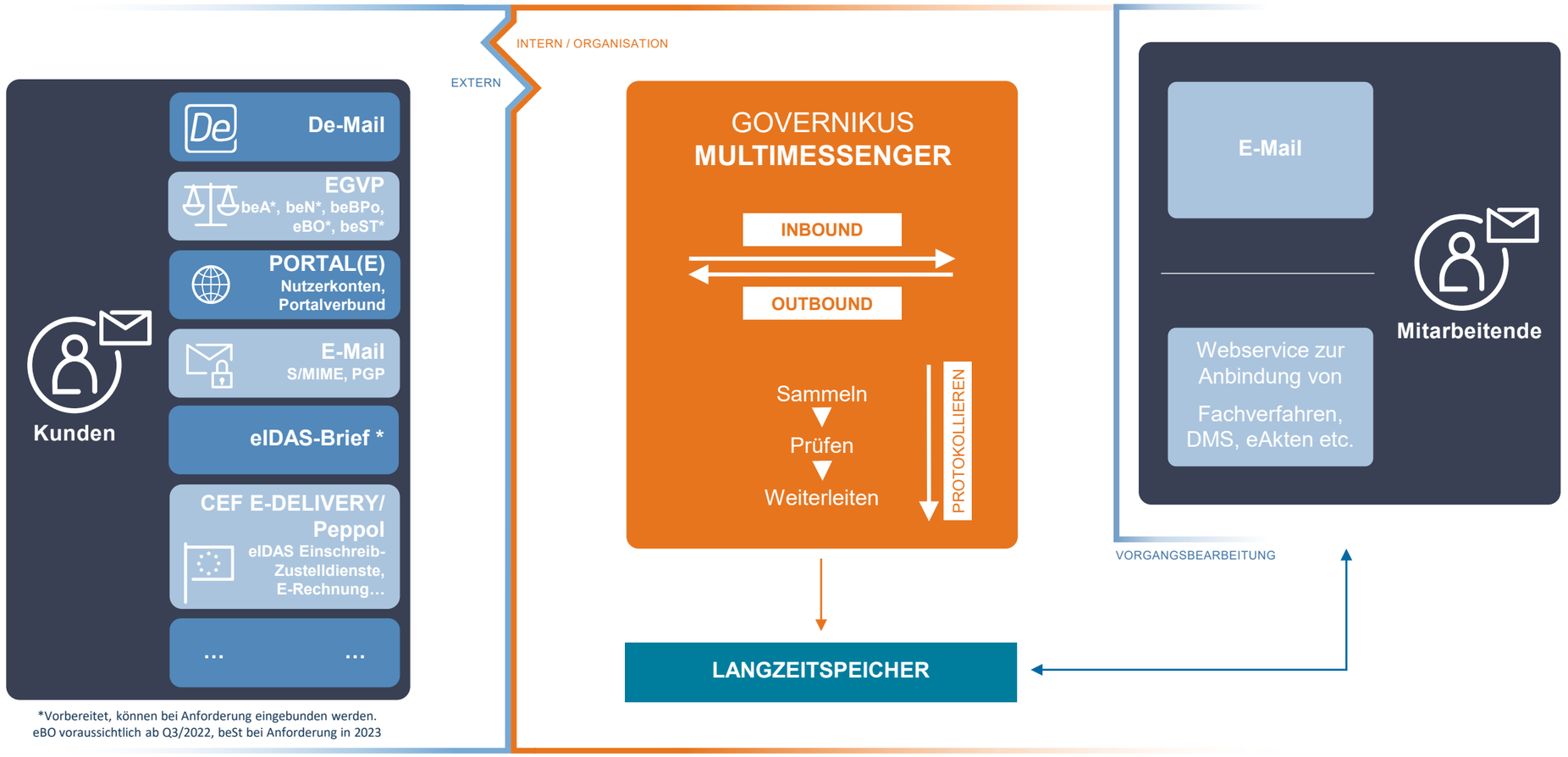
Produkt des IT-Planungsrates

Governikus MultiMessenger wird als Produkt des IT-Planungsrates kontinuierlich gepflegt und in Abstimmung mit Bund und Ländern weiterentwickelt.

Die jeweils gültige Übersicht der Beitritte finden Sie unter:
www.governikus.de/loesungen/it-planungsrat/anwendung-governikus-multimessenger/

Produkte des IT-Planungsrates
... sind IT-Lösungen, die aus Projekten oder projektähnlichen Strukturen des IT-Planungsrats hervorgegangen sind und nun gemeinsam genutzt, dauerhaft betrieben und weiterentwickelt werden. (www.it-planungsrat.de)

Funktionalitäten



Verarbeitung Multikanal

Governikus MultiMessenger (kurz GMM) ist eine Multikanalkommunikationsplattform, die alle in der öffentlichen Verwaltung relevanten Nachrichten-Transportkanäle und alle elektronischen Einschreib-Zustelldienste technisch-juristisch verarbeiten kann. Für die Bearbeitung bzw. den Eingang in eine eAkte-Lösung ist es unerlässlich, dass die eingehenden Nachrichten mit ihren unterschiedlichen Ausprägungen auch hinsichtlich der Authentizität, Integrität und Rechtsverbindlichkeit korrekt empfangen und geprüft werden, bevor sie an eAkte oder beweiswerterhaltende Langzeitspeicherung übergeben werden. Notifizierte deutsche Einschreibzustelldienste sind aktuell De-Mail und eIDAS-Brief. Über den Peppol-Kanal kann GMM auch elektronische Rechnungen gemäß gesetzlicher Vergaben und Spezifikationen empfangen.

Jede von GMM entgegengenommene elektronische Nachricht wird vereinheitlicht, geprüft und protokolliert sowie im gewünschten Format an das jeweils zuvor definierte interne System bzw. an den relevanten externen Empfänger weitergesendet. Die Originalformate bleiben dabei vollständig erhalten und können für die Beweiswerterhaltung direkt über eine standardisierte Schnittstelle gemäß Technischer Richtlinie 03125 (TR-ESOR) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in einen Langzeitspeicher übergeben werden.

Die Anbindung an beispielsweise DATA Aeonia ist dabei optional direkt an GMM oder erst später an der eAkte möglich.

Durchlaufene Prozessschritte sowie die entsprechenden Prüfergebnisse werden in einem Laufzettel protokolliert, der Nachricht zugeordnet und im sog. Poststellenbuch vermerkt. Eine lückenlose Nachweisbarkeit ist somit gewährleistet.

Kommunikationswege

Nachrichtenkanäle
GMM nimmt elektronische Nachrichten aus dem jeweiligen angebundenen Quellsystem entgegen und überführt sie in ein einheitliches Format. Die Originalformate bleiben aber vollständig erhalten. Dabei kann es sich beispielsweise um folgende Nachrichtenkanäle bzw. -formate handeln:

- E-Mail (verschlüsselt und unverschlüsselt)
- De-Mail
- eIDAS-Brief
- EGVP/OSCI
- Besondere Postfächer, gemäß elektronischem Rechtsverkehr (beBPo, beA, beN, eBO, beSt …)
- Webportale, Service- bzw. Nutzerkonten, Fachverfahren mittels Webservice-Schnittstelle basierend auf XTA
- EU – elektronische Einschreib-Zustelldienste, CEF eDelivery/Peppol (u.a. für E-Rechnung)

Grundsätzlich unterscheidet GMM im Rahmen der Nachrichtenverarbeitung und -weiterleitung zwischen Inbound, Outbound und internen Nachrichten.

Inbound-Nachrichten
GMM empfängt über die unterschiedlichen externen Eingangskanäle alle eingehenden elektronischen Nachrichtenformate. Die Nachrichten werden geprüft und intern in das jeweils gewünschte Zielsystem zur Vorgangsbearbeitung weitergeleitet. Als Zielsystem können flexibel Fachverfahren, DMS- oder eAkten-Systeme sowie das intern verwendete E-Mail-System angebunden werden. Die eindeutige Zuordnung der internen Empfänger wird dabei über virtuelle Postfächer festgelegt.

Outbound-Nachrichten
Ausgehende elektronische Nachrichten, die direkt intern aus einem angebundenen Fachverfahren, eAkten-System oder aber von einem internen E-Mail-Server versendet werden, nimmt GMM entgegen und leitet sie nach Ablauf der Prüfroutinen an das gewünschte Kommunikationssystem des externen Empfängers weiter. Dabei wird die Nachricht in das Zielformat übersetzt und die explizite Zugangseröffnung unterstützt. Möchte Ihr Kommunikationspartner also von Ihnen lediglich via De-Mail kontaktiert werden, sorgt GMM dafür, dass – egal aus welchem Ihrer Systeme Sie ihm eine Nachricht zukommen lassen – dieser die Nachricht auch via De-Mail erhält. Die Identitäten der externen Empfänger:innen werden im internen Identitäten-Speicher verwaltet.

Features

Virtuelle Postfächer (VPF)
Für die Nachrichtenverarbeitung, -prüfung und -weiterleitung werden in GMM virtuelle Postfächer definiert, die in hierarchische Funktions- oder Gruppenpostfächer zusammengefasst werden. Diese VPF dienen der Weiterleitung in die gewünschten Zielsysteme. Die Konfiguration der Quell- und Zielsysteme, die Prüfroutinen, Weiterleitungsbestätigungen, Fehlerbenachrichtigungen für Dateiformate, Virenschutz etc. werden über diese VPF kundenindividuell gesteuert. Anders als bei Postfächern, in denen Nachrichten für beliebige spätere Zugriffe vorgehalten werden, übergibt GMM aktiv Nachrichten an ein Zielsystem („Push"-Mechanismus). Nachrichten verbleiben nur für die Dauer der Verarbeitung und im Fehlerfall im virtuellen Postfach bzw. GMM.

Ver- und Entschlüsselung
Die Ver- und Entschlüsselungen von Nachrichten werden zentral durch GMM bei der Übergabe in die Zielsysteme veranlasst bzw. direkt in GMM vorgenommen. Die dafür erforderlichen Schlüssel werden im GMM-internen Identitätenspeicher verwaltet.

Verschlüsselte Nachrichten können entweder PGP- oder S/MIME-verschlüsselte E-Mails, EGVP- oder OSCI-Nachrichten, De-Mails oder eIDAS-Briefe sein.

Verifikation von Signaturen und Zeitstempeln
Die Prüfung von Signaturzertifikaten und Zeitstempeln eingehender Nachrichten und Anhänge wird zentral über GMM gesteuert und veranlasst. GMM greift dabei auf Komponenten des Produkts des IT-PLR Anwendung Governikus zu. Die Verifikationskomponenten der Anwendung Governikus werden kontinuierlich gemäß aktueller Marktgegebenheiten und gesetzlicher Anforderungen gepflegt und weiterentwickelt. Somit ist auch die Prüfung europäischer Formate, beispielsweise gemäß der eIDAS-Verordnung, gewährleistet.

Laufzettel
Die Prüfergebnisse werden übersichtlich und optisch aufbereitet in einem barrierefreien sog. Laufzettel dargestellt. Dieser wird der entsprechenden Nachricht als Anhang beigefügt. Mitarbeitende innerhalb einer Organisation müssen also keine technischen Prüfungen manuell vornehmen oder veranlassen. Sie benötigen weder Spezialwissen über Zertifikate noch zusätzliche Clientanwendungen, haben aber dennoch die Gewissheit über das Prüfergebnis. Darüber hinaus können die Prüfergebnisse mit der Original-Nachricht zur Langzeitaufbewahrung an ggf. angeschlossene TR-ESOR-Systeme (beispielsweise DATA Aeonia) übergeben werden.

Features

Verwaltung von digitalen Identitäten, Zertifikaten und Zugangseröffnung
GMM verfügt über einen integrierten Identitätenspeicher. In diesem werden die für die Ver- und Entschlüsselung benötigten Schlüssel aller Kommunikationspartner:innen hinterlegt. Ebenfalls verwaltet wird in dem Identitätenspeicher die explizite Zugangseröffnung mit dem bevorzugten Kommunikationsweg des externen Kommunikationspartners.
Darüber hinaus können über eine offene und standardisierte Schnittstelle (SPML) auch externe Identitätsmanagementlösungen angebunden werden.

Die komplexen und aufwendig zu pflegenden Aufgaben hinsichtlich des Schlüsselmanagements sowie der Zugangseröffnung können somit über GMM zentralisiert werden. Das erleichtert innerhalb Ihrer Organisation den Umgang mit elektronischer Kommunikation erheblich und steigert die Akzeptanz bei Ihren Mitarbeitenden.

Virenprüfung
Um eingehende Nachrichten und ihre Anhänge direkt auf Viren zu prüfen, können externe Virenprüf-Systeme über eine generische Schnittstelle an GMM angebunden werden. Die Prüfung wird von GMM veranlasst, die Ergebnisse im Laufzettel und im Poststellenbuch vermerkt.

Interne Zustellung in Vorgangsbearbeitungssystemen
Die Weiterleitung von Nachrichten in die interne Infrastruktur erfolgt je nach Konfiguration und Szenario in ein Fachverfahren, DMS- oder eAkten-System. Manche Nutzende bevorzugen die Zustellung in ihrem E-Mail-System. Die Einstellungen werden für jedes im GMM angelegte virtuelle Postfach individuell vorgenommen.

Protokollierung
Alle Informationen und durchgeführten Aktionen zu einer Nachricht werden in einem Laufzettel zusammengefasst. Anhand dieses Laufzettels können interne Empfänger:innen einer Nachricht sämtliche technische und juristische Prüfergebnisse einsehen und so direkt erkennen, ob eine Nachricht bearbeitet werden kann. In den Details werden die Prüfergebnisse zum Absender, Signaturniveau, Verschlüsselung, Format, Schriftformersatz, Virenscan etc. dargestellt.

Die Laufzettel werden auch im Poststellenbuch den jeweiligen Nachrichten beigefügt. Darüber hinaus können diese auch direkt mit der Nachricht an die Langzeitspeicherung übergeben werden.

Die Laufzettel können je nach Konfiguration als PDF und im XML-Format erzeugt und übergeben werden. Für Empfänger:innen über den internen Zustellkanal in das E-Mail-System empfiehlt es sich, den Laufzettel als PDF-Anhang der Nachricht beizufügen. Zur Übergabe in Fachverfahren, DMS- und eAkten-Systeme können die Metadaten im XML-Format übergeben werden.

Optional
Beweiswerterhaltung
Zur frühzeitigen Beweiswertsicherung bzw. -erhaltung können eingehende Nachrichten direkt über die in der TR-ESOR definierte Schnittstelle S.4 im Originalformat an ein System für die Langzeitaufbewahrung übergeben werden. Die von GMM erzeugte Nachrichten-ID wird dabei mit übergeben. Die TR-ESOR-konforme Lösung Governikus DATA Aeonia verwendet die übergebene Nachrichten-ID dabei als AOID (ebenfalls in der TR spezifiziert). Über die Nachrichten-ID bzw. AOID werden sämtliche Nachrichten von den angeschlossenen Systemen, beispielsweise eAkte oder sonstige Fachverfahren, referenziert.

Umfangreiche Tools zur Administration

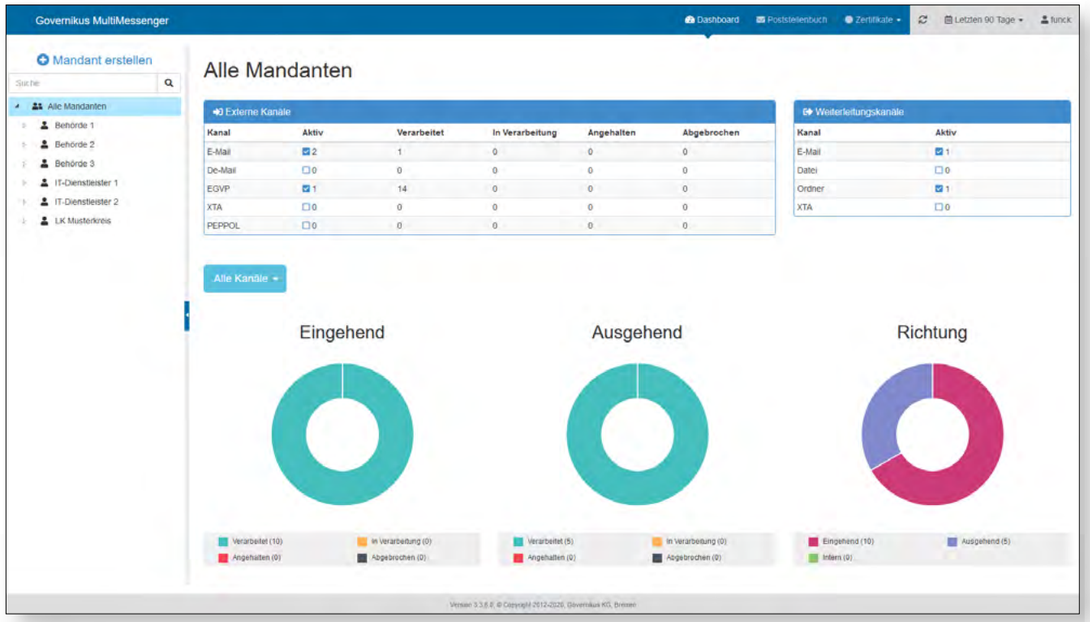
Webclient

Für die Administration steht mit dem GMM Webclient ein einfach zu bedienendes Administrationstool zur Verfügung. Die webbasierte Administrationsoberfläche ermöglicht die einfache Konfiguration der virtuellen Postfächer, bietet über ein übersichtliches Dashboard wichtige Verkehrszahlen, erlaubt Zugriffe auf alle wichtigen Metainformationen des Poststellenbuches und gewährt Zugang und Überblick über die Zertifikatsverwaltung.

Die Authentisierung am Webclient erfolgt über ein Windows-Benutzerkonto, das der lokalen Benutzergruppe bzw. der Active Directory-Benutzergruppe der GMM-Administrator:innen zugeordnet ist. Unterschieden wird dabei zwischen System- und Fachadministration, auch für unterschiedliche Organisationen. Damit können die Zugriffsrechte für unterschiedliche Mandanten gesteuert werden.

VPF- und Organisationsstruktur

Über eine frei konfigurierbare Baumstruktur können beliebige Organisationsstrukturen und zugeordnete virtuelle Postfächer (VPF) angelegt und konfiguriert werden. Dies erlaubt auch die Verwaltung voneinander unabhängiger Organisationsstrukturen, die wiederum logisch unterteilt werden können, beispielsweise zur Abgrenzung von Fachbereichen oder Abteilungen. Auch die Anzeigen des Dashboards und des Poststellenbuches können hierüber gesteuert werden. Die vereinfachte Auswertung der Verkehrszahlen ist dadurch ebenfalls möglich.



Dashboard

Über das GMM-Dashboard behalten Administrator:innen jederzeit den Überblick über die gesamte elektronische Kommunikation, je nach Zugriffsberechtigung für Fach- oder Mandanten-Administration. System-Administrator:innen haben zudem Zugriff auf alle Konfigurationsdateien.

Das Dashboard aggregiert die Anzahl der verarbeiteten Nachrichten und bietet mit der Aufschlüsselung nach Kanal und Verarbeitungsstatus einen umfassenden und schnellen Überblick über den aktuellen Zustand der Poststelle bzw. den aktuellen Status der Nachrichtenverarbeitung. Per Mausklick kann dies auch differenziert für einzelne VPF oder VPF-Gruppen angezeigt werden.

In Übersichtstabellen wird der Nachrichtendurchsatz pro externem Kanal und Weiterleitungskanal angezeigt. Mit interaktiven Kreisdiagrammen wird, unterteilt nach Verarbeitungsstatus, die Anzahl der ein- und ausgehenden Nachrichten visualisiert.

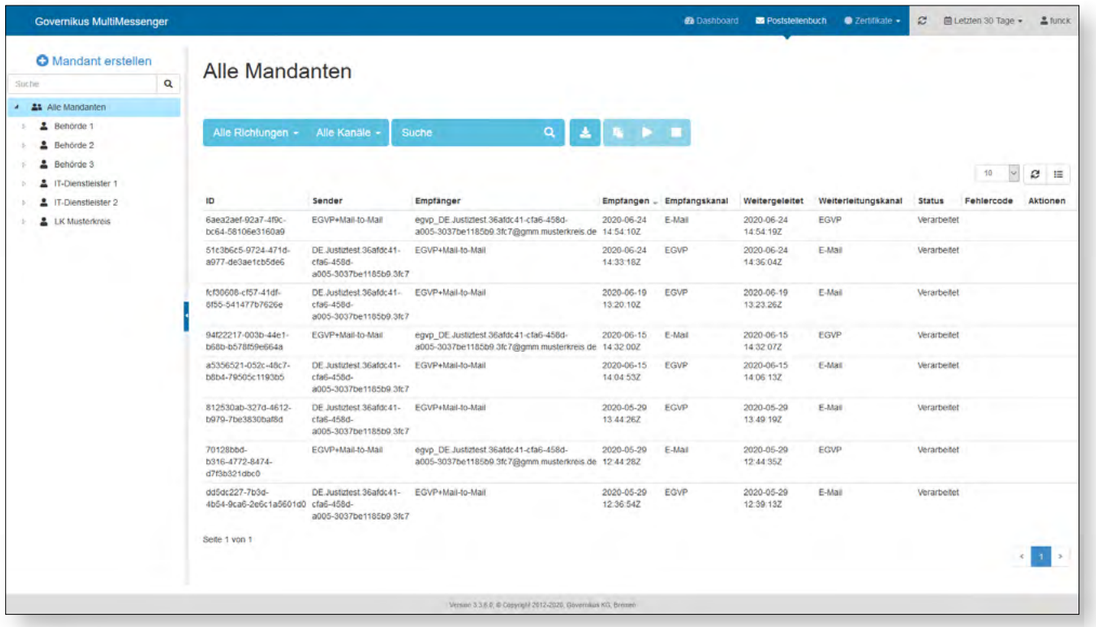
Poststellenbuch

GMM protokolliert alle Nachrichten in einem Poststellenbuch. Das exportierbare Poststellenbuch ermöglicht eine mandantengenaue Zuordnung und Abrechnung für die unterschiedlichen Kommunikationskanäle.

Darüber hinaus bietet das Poststellenbuch Zugriff auf alle wichtigen Metainformationen sämtlicher Nachrichten sowie die zugehörigen Laufzettel mit sämtlichen Prüfergebnissen und ermöglicht im Fehlerfall den Zugriff auf die Originalnachricht und das Fehlerprotokoll.

Im Poststellenbuch werden sämtliche zu einer Nachricht gehörenden Informationen, durchgeführte Aktionen sowie erstellte Laufzettel gespeichert und können über den Webclient aufgerufen werden.

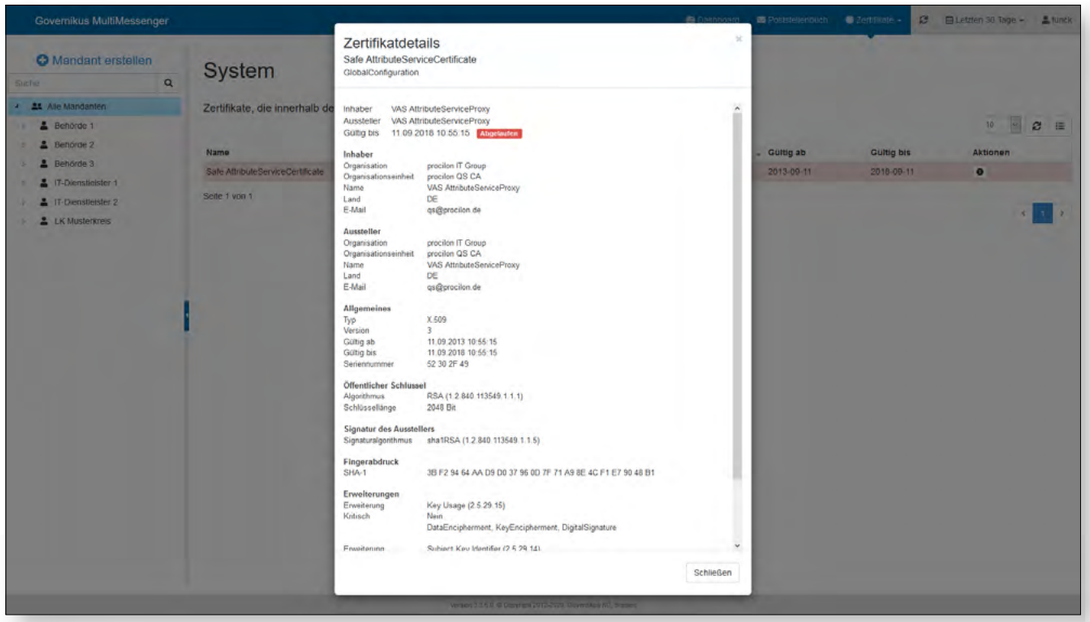
Umfangreiche Filter- und Sortierfunktionen erleichtern das Auffinden von Nachrichten; je VPF können individuelle, automatisierte Löschfristen eingestellt werden. Darüber hinaus lassen sich über das Poststellenbuch Nachrichten anhalten und auch wieder in die Weiterverarbeitung überführen.

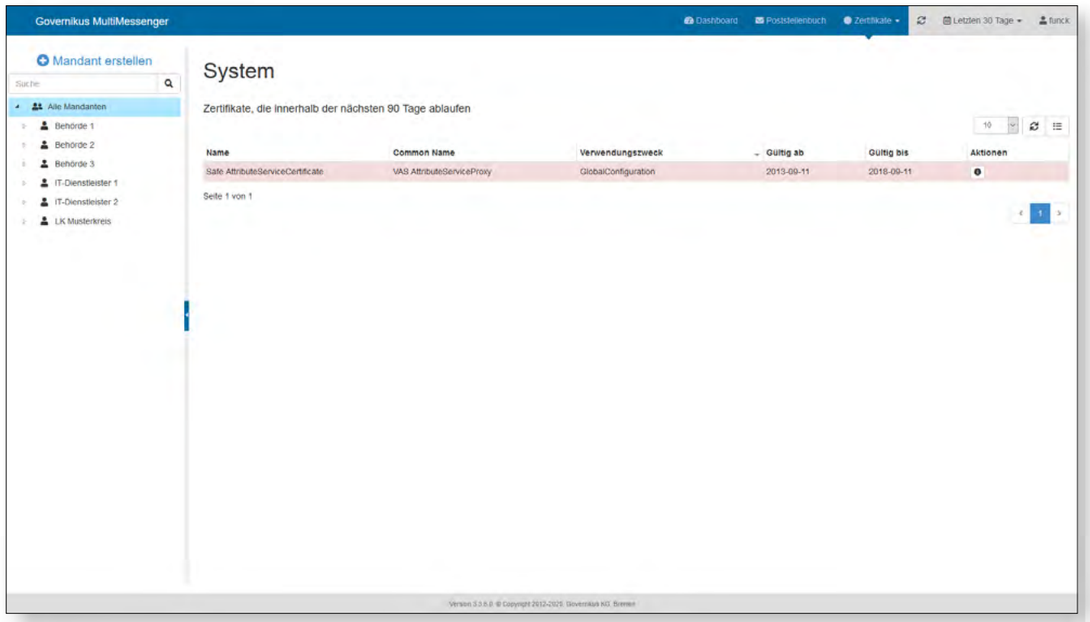


Zertifikatsverwaltung

Administrator:innen erhalten über den Webclient einen umfassenden Überblick über sämtliche im System verwendeten Zertifikate (PGP, S/MIME, EGVP-Schlüssel etc.), können diese einsehen und bei Bedarf austauschen. Darüber hinaus können die im System selbst konfigurierten Zertifikate angezeigt werden.

Ebenso erhalten Administrator:innen über eine filterbare Liste einen schnellen Überblick über Ablaufdaten von Zertifikaten, so dass neue Zertifikate beschafft und ausgetauscht werden können.

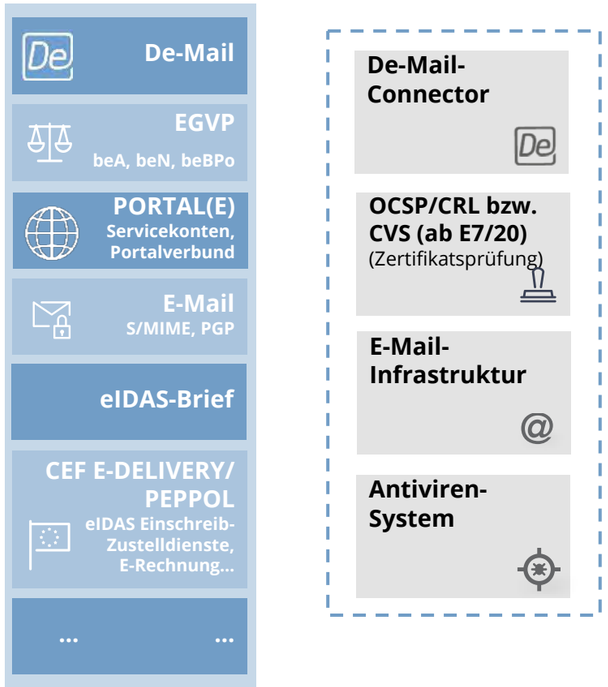




Betriebsumgebung und Systemanforderungen

GMM basiert auf Microsoft .NET-Technologie und erfordert den Einsatz von Microsoft Windows Server 2016 oder 2019. Geplant ist, GMM künftig auch plattformunabhängig betreiben zu können.

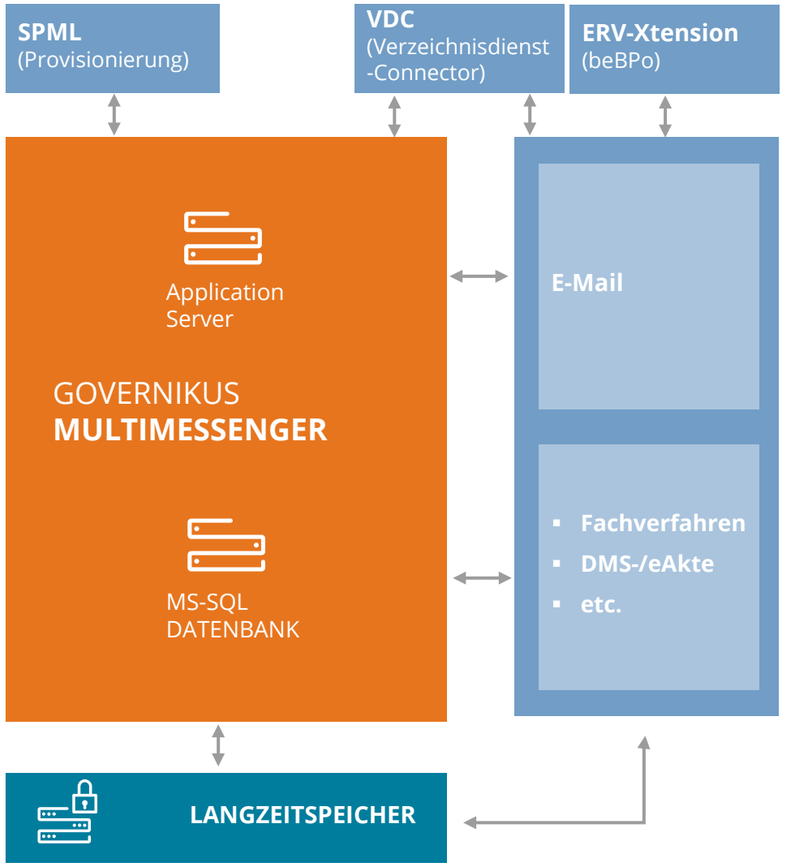
Für die Datenspeicherung wird ein Microsoft SQL-Server 2016 oder 2017 benötigt, kleinere Testszenarien können auch mit Microsoft SQL Express (keine zusätzlichen Lizenzkosten) abgebildet werden. Für das verwendete und auf JAVA basierende Adapter-Framework, das beispielsweise auch den Zugriff auf die Governikus Signatur-Prüfkomponenten ermöglicht, wird JBoss Enterprise Application Platform (EAP) benötigt. Falls Sie JBoss EAP nicht bereits im Einsatz und lizenziert haben, kann der GMM durch eine „embedded JBoss EAP"- Lizenz ergänzt werden.



Für den Empfang und Versand von De-Mails wird ein De-Mail-Connector verwendet, um über eine besonders gesicherte Verbindung direkt auf den Postfach- und Versanddienst des De-Mail Providers zuzugreifen. Die erforderliche Software ist De-Mail-Anbieter-spezifisch und wird von den jeweiligen Providern zur Verfügung gestellt.

Um die Gültigkeit von Zertifikaten bei den zuständigen Trustcentern zu validieren, wird der Certificate Validation Service (CVS) des Governikus-Produkts DATA Varuna benötigt.

Mit einem einfach zu bedienenden Installations-Assistenten sowie einer umfangreichen Dokumentation können Administrator:innen GMM problemlos installieren, konfigurieren und aktualisieren.



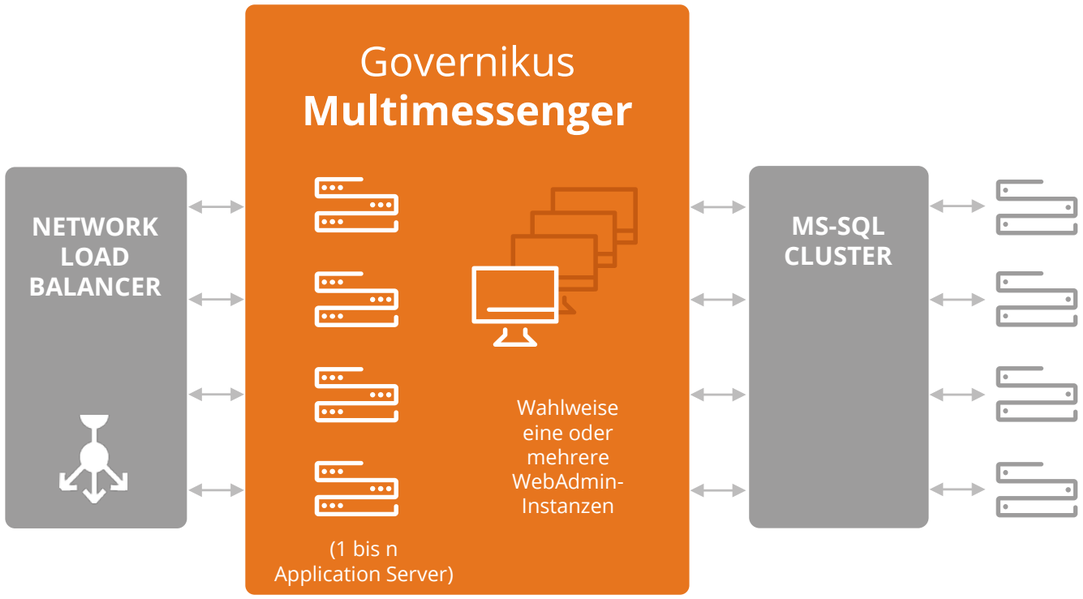
Optional kann GMM Verzeichnisdienstconnector (VDC) für die Suche nach registrierten Nutzern bzw. Identitäten in verschiedenen Verzeichnisdiensten angebunden werden. Hierüber kann beispielsweise nach Adressen im SAFE-Verzeichnis der Justiz, in der GMM Nutzerdatenbank oder im De-Mail-Verzeichnis gesucht werden.

Für die Einbindung in Ihre Infrastruktur stellt VDC zwei komfortable Schnittstellen bereit. Zum einen kann für E-Mail-Infrastrukturen als LDAP-Service ein weiteres Adressbuch hinterlegt werden. Zum anderen ermöglicht eine REST-API die Integration in DMS, wAkten-Systeme oder Fachverfahren.

Mit Governikus SAFE-ID Manager ist es möglich, neue Postfächer im SAFE zu erstellen. Diese werden dann, nach Freischaltung durch einen SAFE-Identitätsadministrator, automatisch in GMM als VPF übernommen.

Skalierbarkeit

GMM ist aus Gründen der Performance und der Ausfallsicherheit höchst skalierbar. Beliebig viele GMM-Instanzen können nebeneinander aufgebaut werden. Gleiches gilt auch für die Datenbank.



Software-anforderungen

Betriebssystem	Microsoft Windows Server 2016 oder 2019
Datenbank	Microsoft SQL Server 2016 oder 2017
Application-Server	Microsoft Internet Information Services (IIS) JBoss Enterprise Application Platform (embedded)
Technologie	JAVA 8

Vorteile
Governikus MultiMessenger

Rechtssicherheit
GMM protokolliert alle Prozessschritte ein- und ausgehender Kommunikation, veranlasst sämtliche Prüfungen und generiert übersichtliche Laufzettel. So können Sie sicher sein, dass Sie jederzeit Zugriff auf rechtlich relevante Informationen zu Ihrer gesamten Kommunikation haben. Darüber hinaus haben Sie die Möglichkeit, alle Nachrichten mit sämtlichen Informationen direkt an einen Langzeitspeicher für die beweiswerterhaltende Langzeitaufbewahrung zu übergeben. Durch die Unterstützung der expliziten Zugangseröffnung können Sie sicher sein, mit Bürger:innen bzw. Kund:innen und Unternehmen auf dem „richtigen“ Weg zu kommunizieren.

Standardisierung
Sämtliche Schnittstellen basieren auf nationalen und internationalen Standards, so dass auf die proprietäre Anbindung von Systemen verzichtet werden kann.

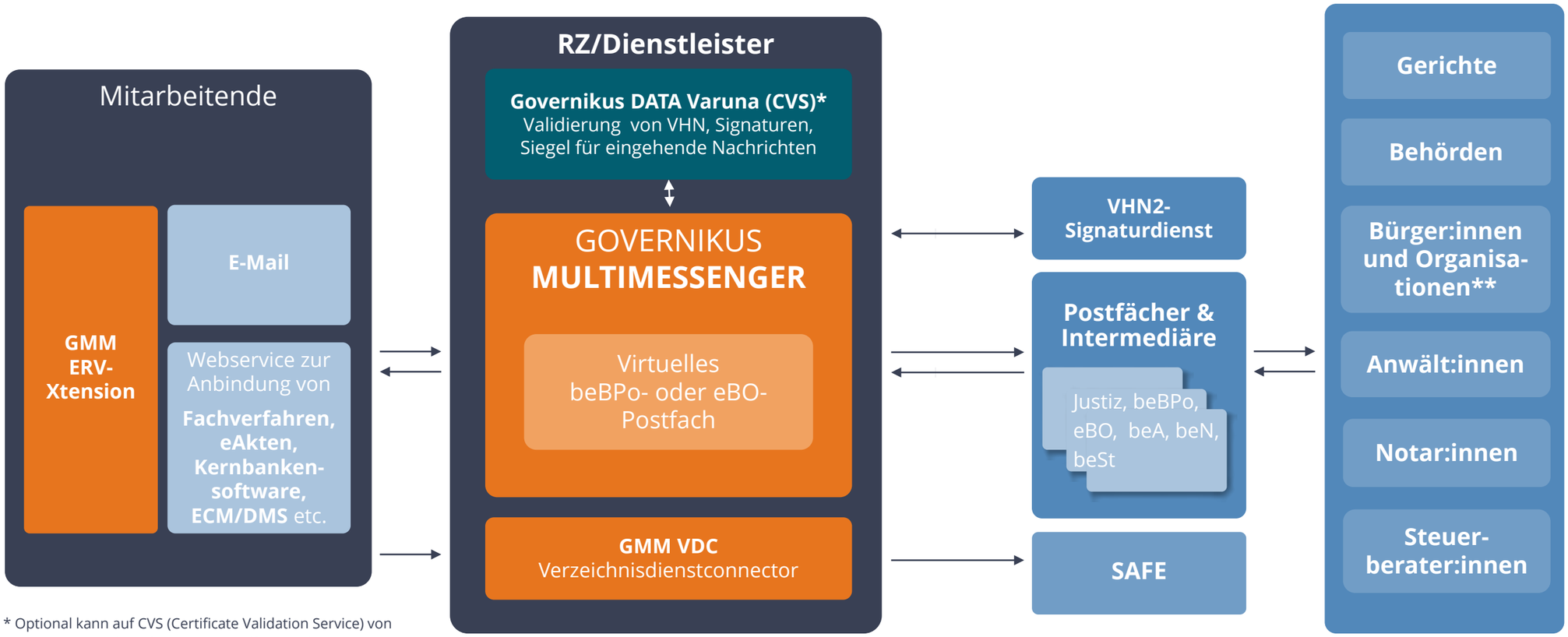
Nutzerakzeptanz und Kundenzufriedenheit
Ihre Mitarbeitenden können einfach und ohne Hintergrundwissen über Kommunikationssysteme, Zertifikatsprüfungen etc. aus ihren bevorzugten und bekannten Systemen (z. B. E-Mail-Client) heraus kommunizieren. Die im Identitätenspeicher hinterlegte Zugangseröffnung ist dabei nur ein Punkt, über den sich Ihre Kolleg:innen keine Gedanken mehr machen müssen. Externe Kommunikationspartner:innen können über den von ihnen präferierten Kanal mit Ihnen kommunizieren.

Effizienz- und Kostenoptimierung
Die Implementierung einer elektronischen Poststelle ermöglicht es Ihnen, sämtliche elektronischen Zustell- und Empfangskanäle zu bedienen und Ihre gesamte Kommunikation ohne Medienbrüche in die etablierten Prozesse und Systeme zu integrieren. Durch die flexible und einfache Handhabung der virtuellen Postfächer können je nach Bedarf präferierte interne Zustellsysteme angepasst werden, ohne in diesen Anpassungen oder Neuinstallationen vornehmen zu müssen.

Zukunftssicherheit / Investitionsschutz
Neue Kommunikationskanäle lassen sich unproblematisch in bestehende Infrastrukturen integrieren und gewähren beispielsweise bei wechselnden oder neuen Anforderungen Anbieterneutralität (z. B. beim Wechsel eines De-Mail-Providers). Dabei ermöglicht GMM, über verschiedene Kanäle zu kommunizieren, ohne zusätzliche Software implementieren zu müssen. Durch die gesicherte Pflege und Weiterentwicklung als Produkt des IT-Planungsrates ist Ihre Investition geschützt.

Mandantenfähigkeit
Aufgrund der Mandantenfähigkeit eignet sich GMM hervorragend für den Betrieb in einem Rechenzentrum. GMM ermöglicht jegliche Art von Abrechnungsmechanismen und eine mandanten- und abteilungsgenaue Zuordnung von Kosten für die unterschiedlichen Kommunikationskanäle.

Elektronischer Rechtsverkehr und GMM



* Optional kann auf CVS (Certificate Validation Service) von Governikus als SaaS zugegriffen werden.

** eBOs können NICHT miteinander kommunizieren

Ein Beispiel für ein Einsatzszenario von Governikus MultiMessenger ist das besondere elektronische Behördenpostfach (beBPo) oder auch das elektronische Bürger- und Organisationenpostfach (eBO). GMM ist u. a. besonders für den Austausch von EGVP/OSCI-Nachrichten geeignet und als sog. ERV-SES (Sende- und Empfangssoftware) im EGVP-Verbund durch die Justiz zugelassen.

Durch die ergänzenden Governikus-Produkte GMM ERV-Xtension, GMM Verzeichnisdienst-connector und SAFE-ID Manager ist GMM eine komfortable Lösung, um am elektronischen Rechtsverkehr teilzunehmen.

Weitere Informationen zu den ergänzenden Produkten finden Sie in einzelnen Infoblättern auf unserer Webseite zum Download: https://www.governikus.de/loesungen/produkte/multimessenger/

Die Umsetzung des beBPo zur Weiterleitung in einen E-Mail-Client bieten wir auch als Service an. Informationen hierzu finden Sie ebenfalls auf unserer Webseite: https://www.governikus.de/loesungen/produkte/bebpo-as-a-service/

Über Governikus

Wir von Governikus haben eine Vision: Wir treten für digitale Souveränität in einer komplex vernetzten Welt ein. Seit über 20 Jahren sorgen aktuell über 200 engagierte Governikus-Mitarbeitende für den Schutz personenbezogener Daten mit unseren sicheren und zukunftsweisenden IT-Lösungen. Wir sind davon überzeugt: Digitalisierung braucht Kryptografie! Sichere Identitäten, vertrauliche und rechtssichere Kommunikation sowie der Umgang mit schützenswerten Daten zur Authentizitäts- und Integritätssicherung stehen hierbei im Vordergrund. Als Pioniere im eGovernment und eJustice gehören gesetzliche Anforderungen, Normen und Standards zu den Grundpfeilern unserer Entwicklungen und Dienstleistungen. Know-how, das im Zuge der fortschreitenden Digitalisierung in weiteren Branchen, wie z. B. dem Gesundheitsmarkt oder im Bereich der Finanzwelt benötigt und geschätzt wird. Wichtig ist uns, auf einen konsequenten Dialog mit Kund:innen und Partner:innen zu bauen.

Wir unterstützen Digitalisierungsvorhaben durch Lösungen, die für gemeinsam nutzbare Basisinfrastrukturen zum Einsatz kommen. Mit den von Governikus entwickelten Produkten des IT-Planungsrats Anwendung Governikus, Anwendung GMM sowie DVDV stehen dem Public Sector und der Justiz (sowie weiteren verwaltungsnahen Institutionen bzw. Organisationen) auf allen föderalen Ebenen wichtige Standardbausteine zur Verfügung. Die Ausweis-App2 des Bundes zur Nutzung der Online-Ausweisfunktion wird ebenfalls von uns entwickelt.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen, Germany
Tel: +49 421 204 95-0
Fax: +49 421 204 95-11
kontakt@governikus.de
www.governikus.de

Niederlassung Berlin
Universitätsstraße 2
10117 Berlin, Germany

Niederlassung Köln
Herwarthstraße 1
50672 Köln, Germany

Niederlassung Erfurt
Johannesstr. 162
99084 Erfurt, Germany


@governikus


@governikus


@governikus


@governikus

governikus.de

Stand Juli 2022