GOVERNIKUS MULTIMESSENGER

Future-proof Multi-Channel Communication

governikus.de

GOVERNIKUS

Future-proof Multi-Channel Communication

Digitalization has long since arrived in communications. Citizens and companies alike are increasingly expecting to be able to communicate electronically with public authorities, the judiciary and other organizations. „Fast and uncomplicated“ is the credo here. At the same time, for reasons of efficiency within organizations, it is essential to integrate electronic communication into their further processing systems without media discontinuity. The introduction of eFiles, as enshrined in the eGovernment and eJustice laws, will only be implemented in a targeted manner if it is possible to exploit the diverse electronic communication potentials and integrate both structured and unstructured communication.

Heterogeneous - National and International Communication Channels

Electronic communication is by no means limited to just one delivery or reception channel. The landscape of communication channels is changing rapidly and becoming increasingly heterogeneous, with the requirements for integrity and authenticity of electronic messages becoming more and more important. New channels will emerge in the coming years without necessarily eliminating existing channels. „One-in one-out“ is therefore not to be expected. The European Union‘s eIDAS regulation will soon add further so-called electronic registered mail delivery services from other European countries, which will have to be received, processed and also readdressed by our administration.

MULTI-CHANNEL
Challenge of our Time

The challenges in dealing with electronic communication are as diverse as the different channels:

- Receiving and delivery channels must be integrated into the existing IT landscape and into a wide variety of business scenarios.
- New standards are emerging that need to be implemented.
- In addition, cryptographically handled messages have to be encrypted and decrypted.
- Along with this, the corresponding certificates have to be managed for different channels.
- The handling of signatures is not limited to the application of the user's own signatures; in accordance with the eIDAS regulation, it must also be possible to verify all European signatures.
- The storage of granted access openings, identities and certificates of the communication partners as well as transparent and legally secure traceability are further points that must be considered.

Whether CIO, system and specialist administration or clerks: Your employees are confronted with these and other challenges every day at various levels. Contrary to the actual objective of digitization, time-consuming and cost-intensive efforts are incurred due to often proprietary isolated solutions with media discontinuities in the processes.

Virtual Mailroom

In order to be able to serve the diverse communication channels within the administration in an efficient and future-proof manner, it is not practical to connect the delivery and reception channels individually to the respective specialist procedures or eFile systems. Instead, it is advisable to establish a central, virtual, electronic mailroom. This can handle all electronic formats, process them and forward them to a desired target system, perform all cryptographic and identity checks and, if necessary, transfer the original messages directly to a long-term storage facility to preserve the value of the evidence. At the same time, it ensures that the access initiated by citizens as well as companies is stored centrally, so that your organization can not only receive electronic communications, but also respond to them in the same way.

To meet the challenge of multi-channel communication, Governikus MultiMessenger (GMM) was developed. The intelligent communication platform offers solutions for future challenges arising from the constant further and new development of digital channels in electronic communication. Digitization of processes, introduction of eFiles as well as integration into existing IT landscapes: The GMM enables a future-proof, overarching multi-channel strategy. As a product of the IT Planning Council, Governikus MultiMessenger is continuously maintained and further developed in coordination with the federal and state governments.

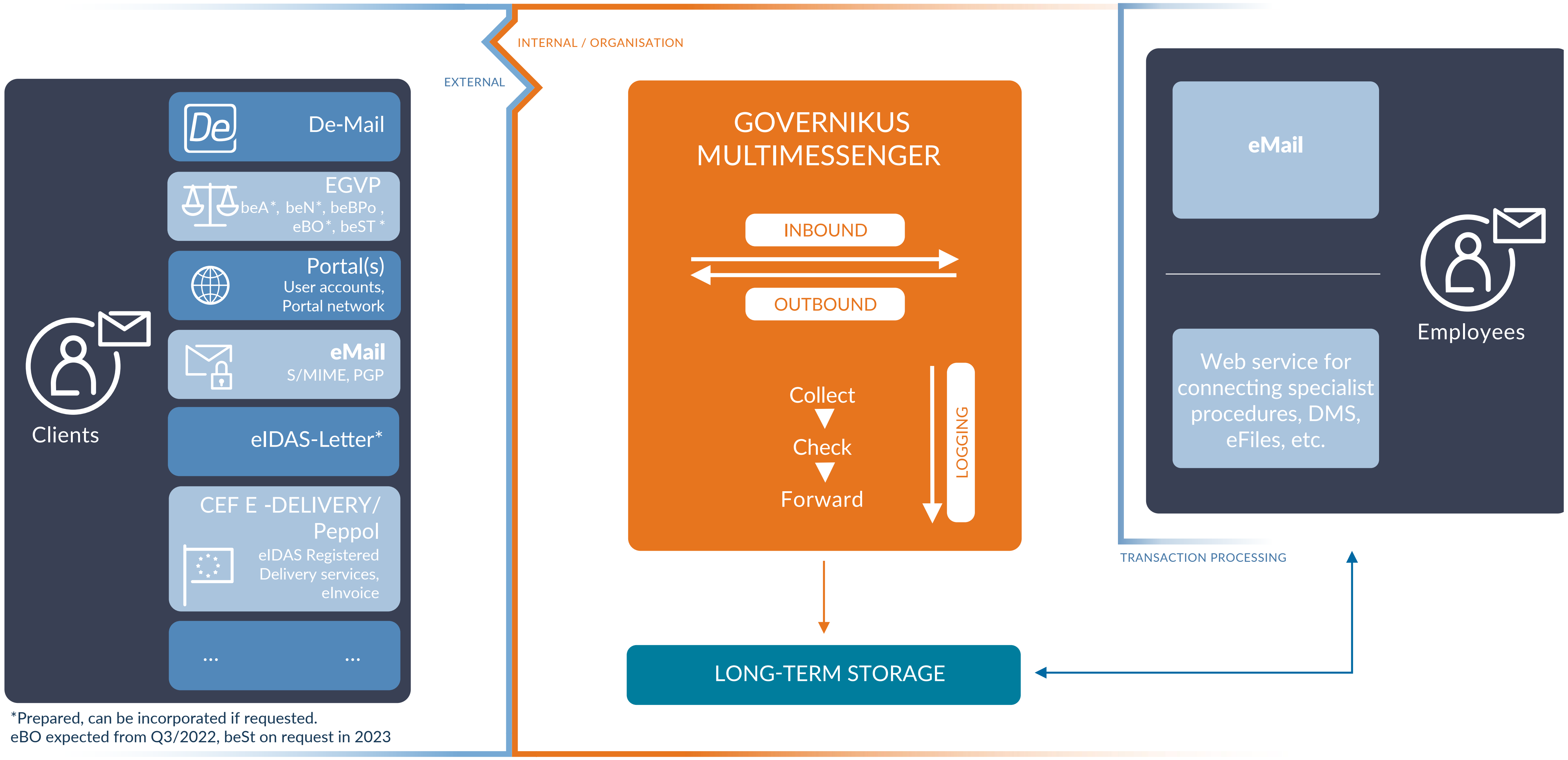
The current overview of the accessions can be found at:

https://www.governikus.de/en/loesungen/it-planungsrat/anwendung-governikus-multimessenger/

i **Products of the IT Planning Council...**
...are IT solutions that have emerged from projects or project-like structures of the IT Planning Council and are now shared, permanently operated and further developed. (https://www.it-planungsrat.de/en/)

THE SOLUTION
Governikus MultiMessenger

Functionalities



*Prepared, can be incorporated if requested.
eBO expected from Q3/2022, beSt on request in 2023

Multichannel Processing
Governikus MultiMessenger (GMM for short) is a multi-channel communication platform that can process all message transport channels relevant in public administration and all electronic registered delivery services in a technical-legal manner. For processing or input into an eFile solution, it is essential that the incoming messages with their different characteristics are also correctly received and checked with regard to authenticity, integrity and legal validity before they are transferred to eFiles or long-term storage for the preservation of evidentiary value. Notified German registered mail delivery services are currently De-Mail and eIDAS letter. GMM can also receive electronic invoices via the Peppol channel in accordance with statutory awards and specifications.

Each electronic message received by GMM is standardized, checked and functionalities logged, and forwarded in the required format to the respective previously defined internal system or to the relevant external recipient. The original formats are fully preserved and can be transferred directly to a long-term storage facility via a standardized interface in accordance with Technical Guideline 03125 (TR-ESOR) of the German Federal Office for Information Security (BSI) for the purpose of preserving probative value. The connection to DATA Aeonia, for example, is optionally possible directly at GMM or later at the eFile.
Process steps that have been carried out and the corresponding check results are logged in a routing slip, assigned to the message and noted in the so-called Post Office Book. This ensures complete traceability.

Communication Channels

Mail Channels

GMM receives electronic messages from the respective connected source system and converts them into a uniform format. However, the original formats remain completely intact. This may involve the following mail channels or formats, for example:

- eMail (encrypted and unencrypted)
- De-Mail
- eIDAS letter
- EGVP/OSCI
- Special mailboxes, in accordance with electronic legal transactions (beBPo, beA, beN, eBO, beSt ...)
- Web portals, service or user accounts, specialized procedures via web service interface based on XTA
- EU - electronic registered mail delivery services, CEF eDelivery/Peppol (e.g. for eInvoice)

GMM basically differentiates between inbound, outbound and internal messages within the scope of message processing and forwarding.

Inbound Messages

GMM receives all incoming electronic message formats via the various external inbound Channels. The messages are checked and forwarded internally to the desired target system for processing. Specialist procedures, DMS or eFile systems as well as the internally used eMail system can be flexibly connected as target systems. The unique assignment of internal recipients is defined via virtual mailboxes.

Outbound Messages

GMM accepts outbound electronic messages sent directly internally from a connected specialized process, eFile system or from an internal eMail server and forwards them to the desired communication system of the external recipient after the check routines have been completed. In the process, the message is translated into the target format and explicit access opening is supported. So if your communication partner only wants to be contacted by you via De-Mail, GMM ensures that - regardless of which of your systems you send him a message from - he also receives the message via De-Mail. The identities of the external recipients are managed in the internal identity store.

Features

Virtual Mailboxes

For message processing, checking and forwarding, virtual mailboxes are defined in GMM, which are grouped into hierarchical function or group mailboxes. These virtual mailboxes are used for forwarding to the desired target systems. The configuration of the source and target systems, the checking routines, forwarding confirmations, error notifications for file formats, virus protection, etc. are controlled on a customer-specific basis via these virtual mailboxes. Unlike mailboxes, which hold messages for any subsequent access, GMM actively delivers messages to a target system („push“ mechanism). Messages remain in the virtual mailbox or GMM only for the duration of processing and in the event of an error.

Encryption and Decryption

The encryption and decryption of messages are initiated centrally by GMM when they are transferred to the target systems or are performed directly in GMM. The keys required for this are managed in the GMM-internal identity store. Encrypted messages can be either PGP or S/MIME encrypted eMails, EGVP or OSCI messages, De-Mails or eIDAS letters.

Verification of Signatures and Timestamps

The verification of signature certificates and time stamps of incoming messages and attachments is controlled and initiated centrally via GMM. GMM accesses components of the IT Planning Council‘s Anwendung Governikus for this purpose. The verification components of the Governikus application are continuously maintained and further developed according to current market conditions and legal requirements. This also ensures the verification of European formats, for example in accordance with the eIDAS regulation.

Processcard

The check results are presented clearly and visually in an accessible so-called processcard. This is attached to the corresponding message. This means that employees within an organization do not have to perform or initiate technical checks manually. They need neither special knowledge about certificates nor additional client applications, but still have the certainty of the check result. In addition, the check results can be transferred with the original message to any connected TR-ESOR systems (such as DATA Aeonia) for long-term storage.

Features

Management of Digital Identities, Certificates and Access Opening

GMM has an integrated identity store. This stores the keys required for encryption and decryption for all communication partners. The explicit access opening with the preferred communication path of the external communication partner is also managed in the identity store. In addition, external identity management solutions can be connected via an open and standardized interface (SPML). The complex and time-consuming tasks regarding key management as well as access opening can thus be centralized via GMM. This considerably simplifies the handling of electronic communication within your organization and increases acceptance among your employees.

Virus Check

To check incoming messages and their attachments directly for viruses, external virus checking systems can be connected to GMM via a generic interface. The check is initiated by GMM, and the results are noted in the processcard and in the mailroom book.

Internal Delivery in Transaction Processing Systems

Depending on the configuration and scenario, messages are forwarded to the internal infrastructure in a specialist procedure, DMS or eFile system. Some users prefer delivery in their eMail system. The settings are made individually for each virtual mailbox created in the GMM.

Logging

All information and actions performed on a message are summarized in a processcard. Using this processcard, internal recipients of a message can view all technical and legal check results and thus directly see whether a message can be processed. The check results for the sender, signature level, encryption, format, written form replacement, virus scan, etc. are displayed in the details.

The processcards are also attached to the respective messages in the post office book. In addition, they can also be transferred directly with the message to long-term storage. Depending on the configuration, the processcards can be generated and transferred as PDF and in XML format. For recipients via the internal delivery channel in the eMail system, it is recommended to attach the processcard as a PDF attachment to the message. The metadata can be transferred in XML format for transfer to specialist processes, DMS and eFile systems.

Preservation of Evidence Value

For early preservation of evidence value, incoming messages can be transferred directly to a system for long-term preservation in their original format via the interface S.4 defined in TR-ESOR. The message ID generated by GMM is also transferred. The TR-ESOR compliant solution Governikus DATA Aeonia uses the transferred message ID as AOID (also specified in the technical guideline). The message ID or AOID is used to reference all messages from the connected systems, such as eFiles or other specialized procedures.

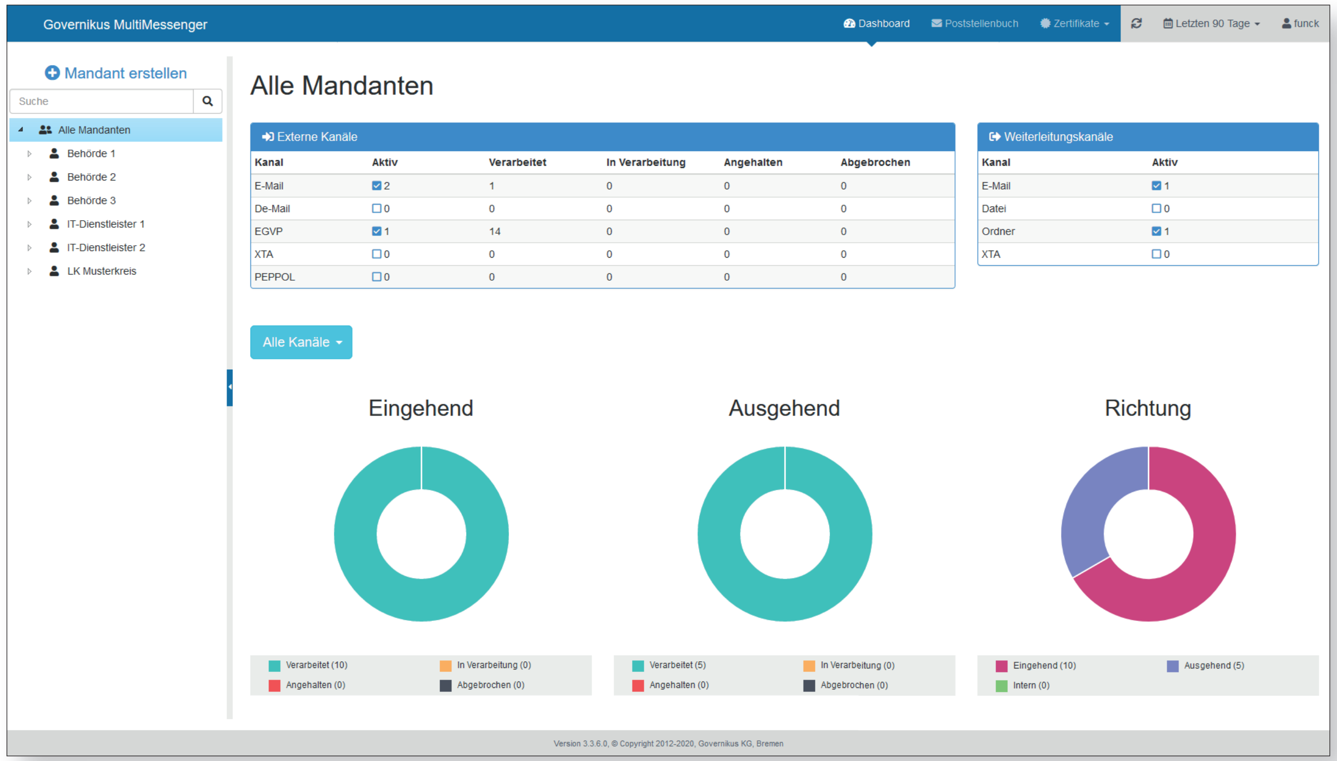
Extensive Tools for Administration

Webclient

The GMM Webclient is an easy-to-use administration tool. The web-based administration interface enables simple configuration of the virtual mailboxes, provides important traffic figures via a clear dashboard, allows access to all important meta information of the mailroom book and grants access and overview of the certificate management. The authentication at the web client is done via a Windows user account that is assigned to the local user group or the Active Directory user group of the GMM administrators. A distinction is made between system and specialist administration, even for different organizations. This allows to control the access rights for different clients.

Virtual Mailboxes and Organizational Structure

Any organizational structures and assigned virtual mailboxes can be created and configured via a freely configurable tree structure. This also allows the management of independent organizational structures, which in turn can be logically subdivided, for example to delineate departments or divisions. The dashboard and mailroom book displays can also be controlled via this. The simplified evaluation of traffic figures is also possible as a result.



Alle Mandanten

Externe Kanäle

Kanal	Aktiv	Verarbeitet	In Verarbeitung	Angehalten	Abgebrochen
E-Mail	☑ 2	1	0	0	0
De-Mail	☐ 0	0	0	0	0
EGVP	☑ 1	14	0	0	0
XTA	☐ 0	0	0	0	0
PEPPOL	☐ 0	0	0	0	0

Weiterleitungskanäle

Kanal	Aktiv
E-Mail	☑ 1
Datei	☐ 0
Ordner	☑ 1
XTA	☐ 0

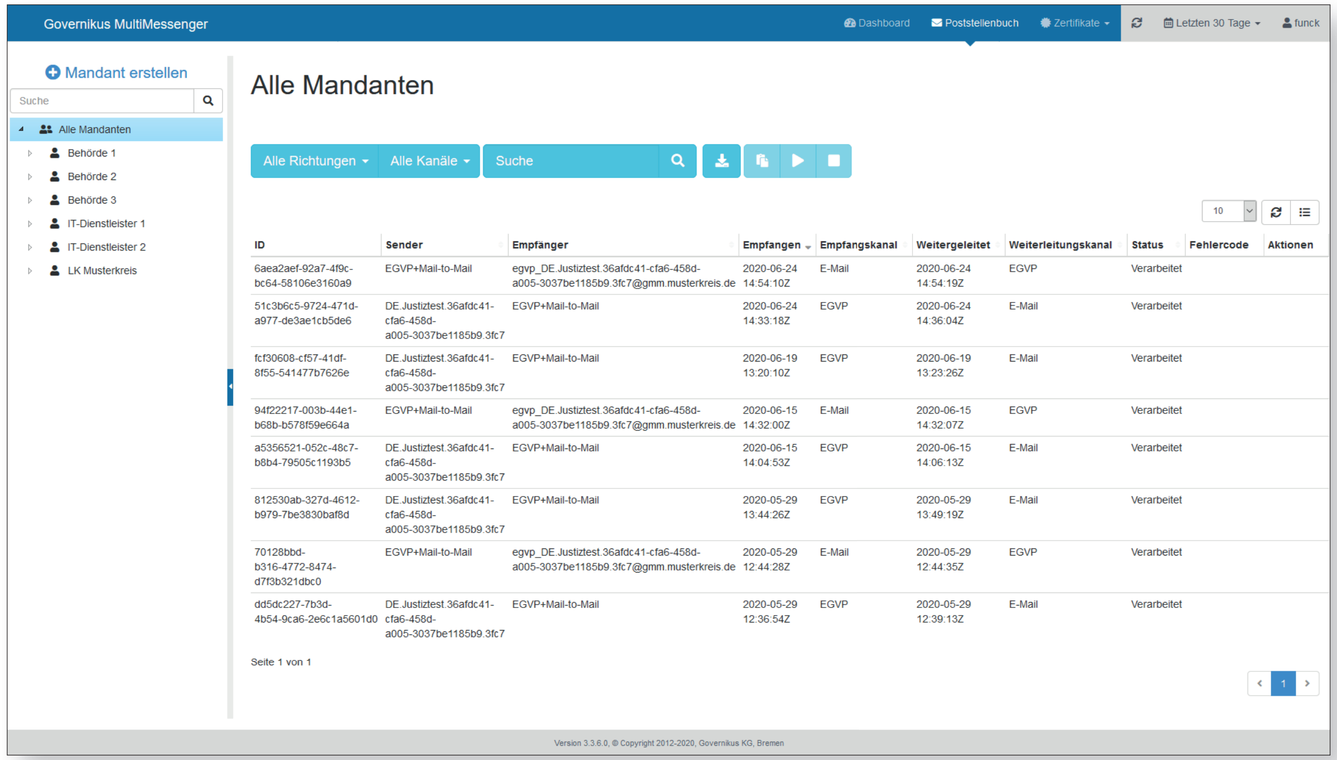
Version 3.3.6.0, © Copyright 2012-2020, Governikus KG, Bremen

Dashboard

The GMM dashboard provides administrators with an overview of all electronic communication at all times, depending on whether they have access rights for specialist or client administration. System administrators also have access to all configuration files. The dashboard aggregates the number of messages processed and, with the breakdown by channel and processing status, provides a comprehensive and quick overview of the current status of the mailroom or the current status of message processing. With a mouse click, this can also be displayed differentiated for individual virtual mailboxes or virtual mailbox groups. Overview tables show the message throughput per external channel and forwarding channel. Interactive pie charts visualize the number of incoming and outgoing messages, subdivided by processing status.

Post Office Book

GMM logs all messages in a post office book. The exportable mailroom book enables client-specific allocation and accounting for the various communication channels. In addition, the mailroom book provides access to all important meta information of all messages as well as the associated processcards with all check results and enables access to the original message and the error log in the event of an error. In the mailroom book, all information belonging to a message, actions performed, and processcards created are stored and can be accessed via the web client. Extensive filtering and sorting functions make it easier to find messages; individual, automated deletion periods can be set for each virtual mailbox. In addition, messages can be stopped via the mailroom book and also transferred back to further processing.



Alle Mandanten

ID	Sender	Empfänger	Empfangen	Empfangskanal	Weitergeleitet	Weiterleitungskanal	Status	Fehlercode	Aktionen
6aea2aef-92a7-4f9c-bc64-58106e3160a9	EGVP+Mail-to-Mail	egvp_DE.Justiztest.36afdc41-cfa6-458d-a005-3037be1185b9.3fc7@gmm.musterkreis.de	2020-06-24 14:54:10Z	E-Mail	2020-06-24 14:54:19Z	EGVP	Verarbeitet		
51c3b6c5-9724-471d-a977-de3ae1cb5de6	DE.Justiztest.36afdc41-cfa6-458d-a005-3037be1185b9.3fc7	EGVP+Mail-to-Mail	2020-06-24 14:33:18Z	EGVP	2020-06-24 14:36:04Z	E-Mail	Verarbeitet		
fcf30608-cf57-41df-8f55-541477b7626e	DE.Justiztest.36afdc41-cfa6-458d-a005-3037be1185b9.3fc7	EGVP+Mail-to-Mail	2020-06-19 13:20:10Z	EGVP	2020-06-19 13:23:26Z	E-Mail	Verarbeitet		
94f22217-003b-44e1-b68b-b578f59e664a	EGVP+Mail-to-Mail	egvp_DE.Justiztest.36afdc41-cfa6-458d-a005-3037be1185b9.3fc7@gmm.musterkreis.de	2020-06-15 14:32:00Z	E-Mail	2020-06-15 14:32:07Z	EGVP	Verarbeitet		
a5356521-052c-48c7-b8b4-79505c1193b5	DE.Justiztest.36afdc41-cfa6-458d-a005-3037be1185b9.3fc7	EGVP+Mail-to-Mail	2020-06-15 14:04:53Z	EGVP	2020-06-15 14:06:13Z	E-Mail	Verarbeitet		
812530ab-327d-4612-b979-7be3830baf8d	DE.Justiztest.36afdc41-cfa6-458d-a005-3037be1185b9.3fc7	EGVP+Mail-to-Mail	2020-05-29 13:44:26Z	EGVP	2020-05-29 13:49:19Z	E-Mail	Verarbeitet		
70128bbd-b316-4772-8474-d7f3b321dbc0	EGVP+Mail-to-Mail	egvp_DE.Justiztest.36afdc41-cfa6-458d-a005-3037be1185b9.3fc7@gmm.musterkreis.de	2020-05-29 12:44:28Z	E-Mail	2020-05-29 12:44:35Z	EGVP	Verarbeitet		
dd5dc227-7b3d-4b54-9ca6-2e6c1a5601d0	DE.Justiztest.36afdc41-cfa6-458d-a005-3037be1185b9.3fc7	EGVP+Mail-to-Mail	2020-05-29 12:36:54Z	EGVP	2020-05-29 12:39:13Z	E-Mail	Verarbeitet		

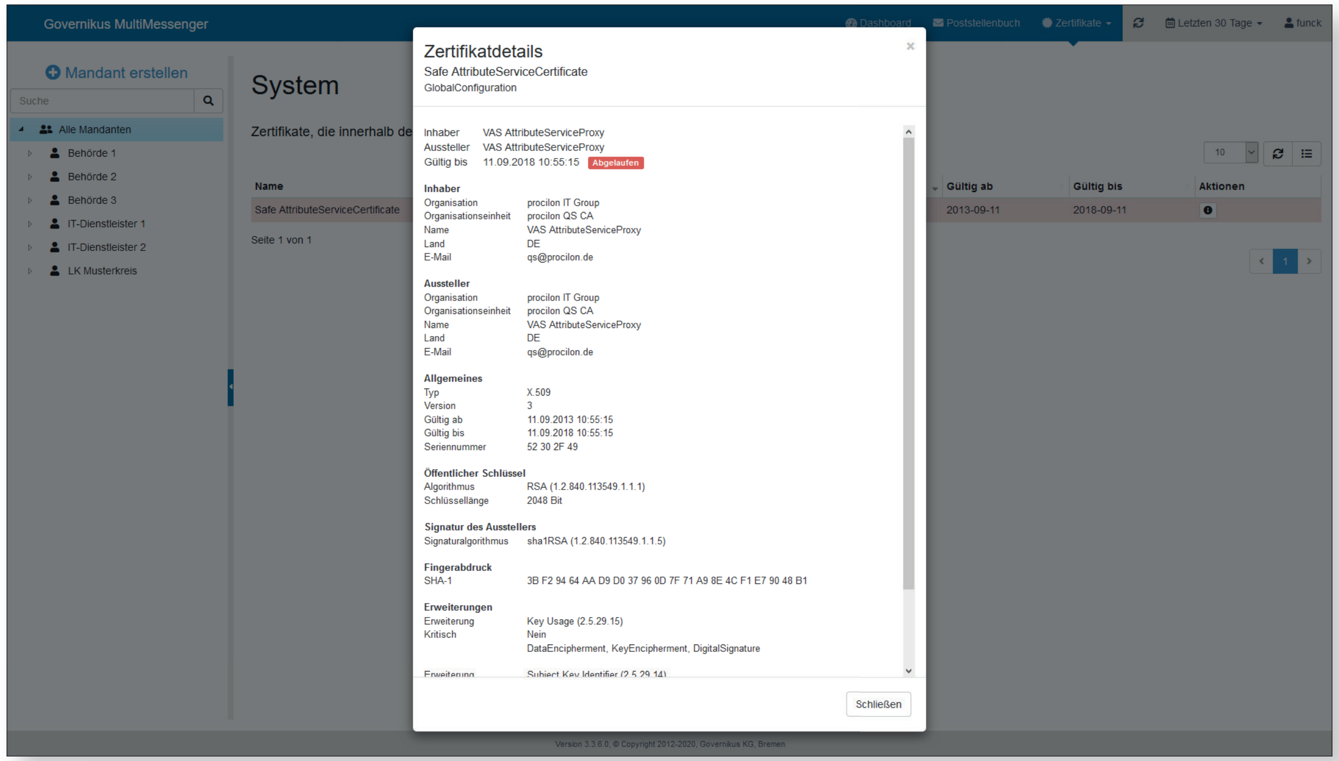
Seite 1 von 1

Version 3.3.6.0, © Copyright 2012-2020, Governikus KG, Bremen

Certificate Management

The web client provides administrators with a comprehensive overview of all certificates used in the system (PGP, S/MIME, EGVP keys, etc.), which they can view and exchange if necessary.

In addition, the certificates configured in the system itself can be displayed. A filterable list also provides administrators with a quick overview of certificate expiration dates so that new certificates can be procured and exchanged.



Zertifikatdetails

Safe AttributeServiceCertificate

GlobalConfiguration

Inhaber	VAS AttributeServiceProxy
Aussteller	VAS AttributeServiceProxy
Gültig bis	11.09.2018 10:55:15 Abgelaufen

Inhaber

Organisation	procilon IT Group
Organisationseinheit	procilon QS CA
Name	VAS AttributeServiceProxy
Land	DE
E-Mail	qs@procilon.de

Aussteller

Organisation	procilon IT Group
Organisationseinheit	procilon QS CA
Name	VAS AttributeServiceProxy
Land	DE
E-Mail	qs@procilon.de

Allgemeines

Typ	X.509
Version	3
Gültig ab	11.09.2013 10:55:15
Gültig bis	11.09.2018 10:55:15
Seriennummer	52 30 2F 49

Öffentlicher Schlüssel

Algorithmus	RSA (1.2.840.113549.1.1.1)
Schlüssellänge	2048 Bit

Signatur des Ausstellers

Signaturalgorithmus	sha1RSA (1.2.840.113549.1.1.5)

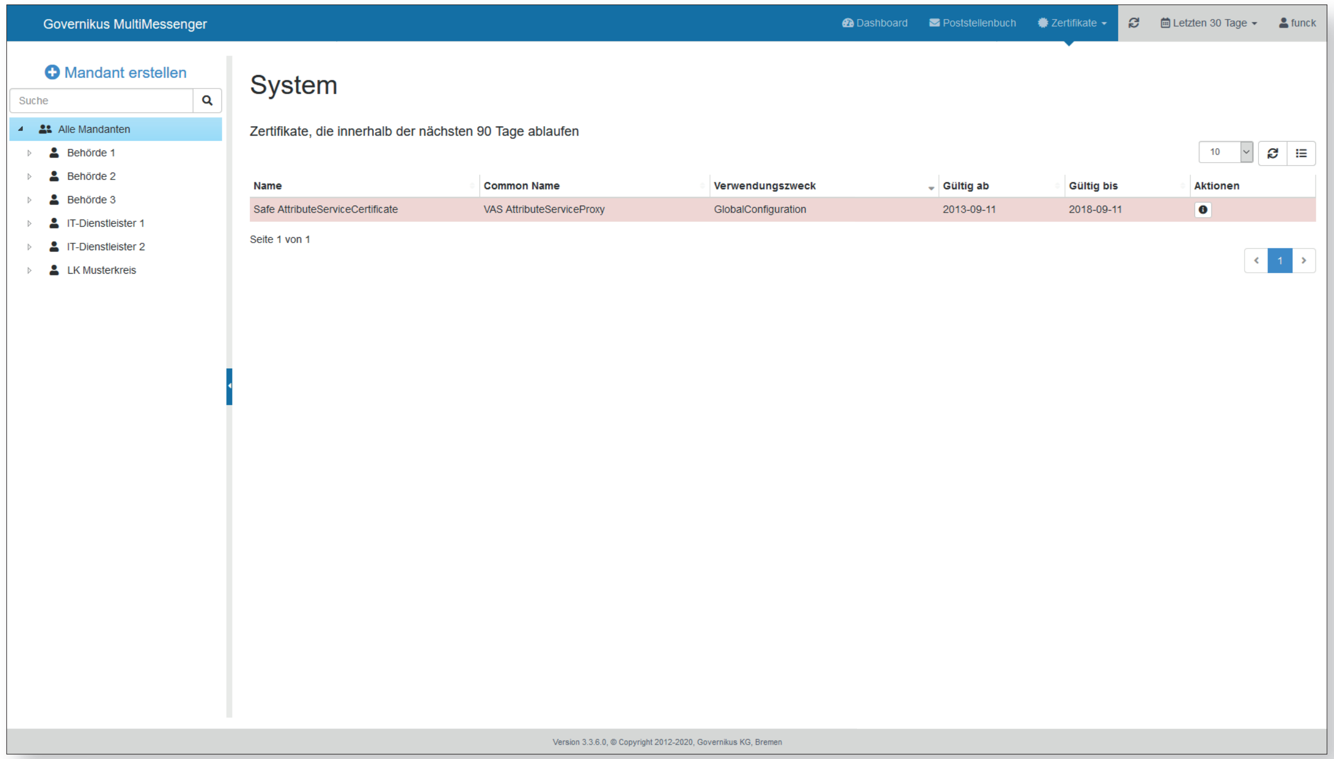
Fingerabdruck

SHA-1	3B F2 94 64 AA D9 D0 37 96 0D 7F 71 A9 8E 4C F1 E7 90 48 B1

Erweiterungen

Erweiterung	Key Usage (2.5.29.15)
Kritisch	Nein
	DataEncipherment, KeyEncipherment, DigitalSignature
Erweiterung	Subject Key Identifier (2.5.29.14)

Version 3.3.6.0, © Copyright 2012-2020, Governikus KG, Bremen



System

Zertifikate, die innerhalb der nächsten 90 Tage ablaufen

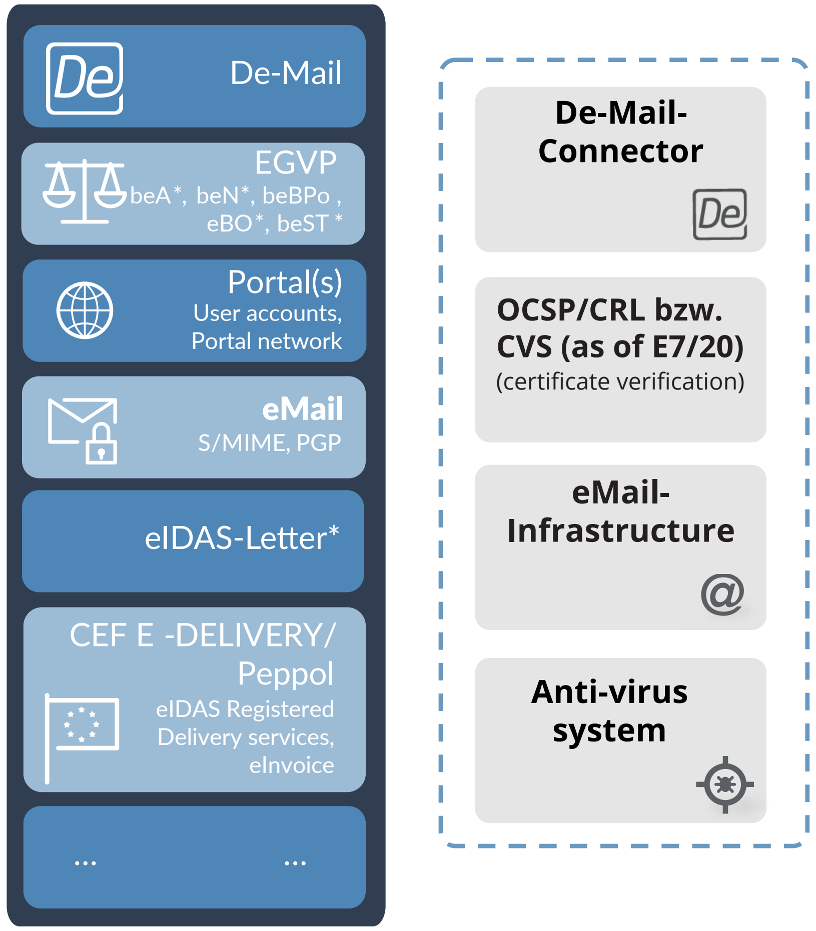
Name	Common Name	Verwendungszweck	Gültig ab	Gültig bis	Aktionen
Safe AttributeServiceCertificate	VAS AttributeServiceProxy	GlobalConfiguration	2013-09-11	2018-09-11	●

Seite 1 von 1

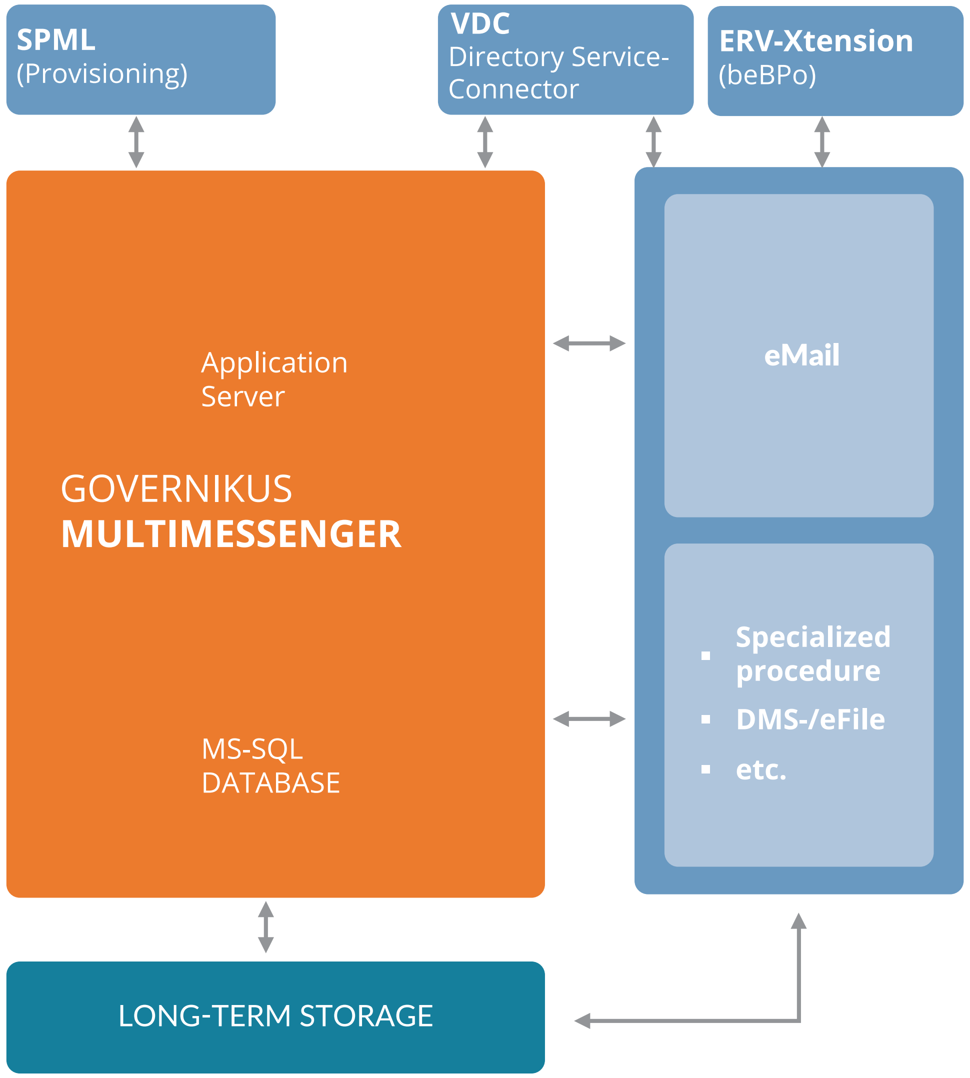
Version 3.3.6.0, © Copyright 2012-2020, Governikus KG, Bremen

Operating Environment and System Requirements

GMM is based on Microsoft .NET technology and requires the use of Microsoft Windows Server 2016 or 2019. It is planned to be able to operate GMM platform-independently in the future. A Microsoft SQL Server 2016 or 2017 is required for data storage, smaller test scenarios can also be mapped with Microsoft SQL Express (no additional license costs). JBoss Enterprise Application Platform (EAP) is required for the JAVA-based adapter framework used, which also enables access to the Governikus signature verification components, for example. If you do not already have JBoss EAP in use and licensed, the GMM can be supplemented by an „embedded JBoss EAP“ license.



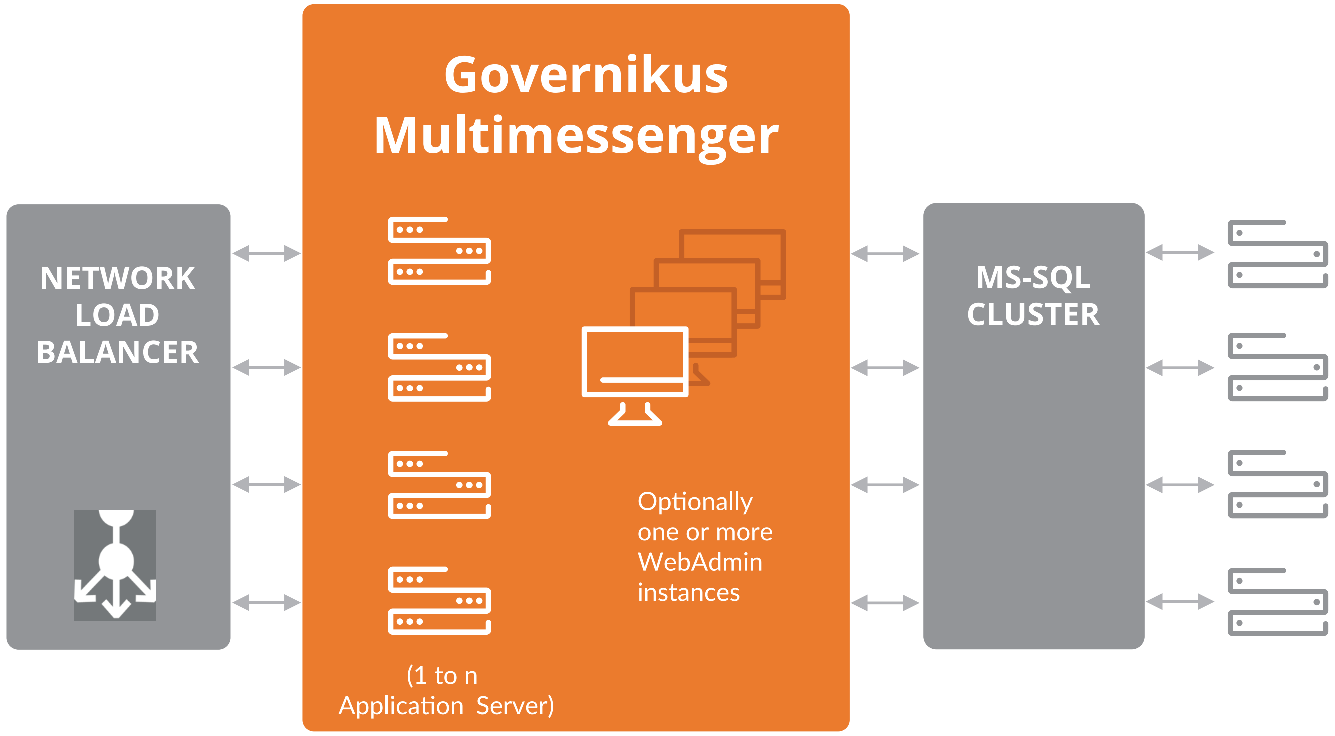
De-Mail
EGVP
beA*, beN*, beBPo , eBO*, beST*
Portal(s)
User accounts, Portal network
eMail
S/MIME, PGP
eIDAS-Letter*
CEF E -DELIVERY/ Peppol
eIDAS Registered Delivery services, eInvoice
... ...
De-Mail-Connector
OCSP/CRL bzw. CVS (as of E7/20)
(certificate verification)
eMail-Infrastructure
Anti-virus system



Optionally, GMM VDC (Directory Service Connector) can be connected to search for registered users or identities in various directory services. This can be used, for example, to search for addresses in the SAFE directory of the justice system, in the GMM user database or in the De-Mail directory. GMM VDC (Directory Service Connector) provides two convenient interfaces for the integration into your infrastructure. On the one hand an additional address book can be stored for eMail infrastructures as LDAP service. On the other hand, a REST API enables integration into DMS, eFile systems or specialized procedures. With Governikus SAFE-ID Manager it is possible to create new mailboxes in SAFE. These are then, after activation by a SAFE identity administrator, automatically transferred to GMM as a virtual mailbox.

Scalability

GMM is highly scalable for performance and reliability reasons. Any number of GMM instances can be set up side by side. The same applies to the database.


NETWORK LOAD BALANCER
Governikus Multimessenger
Optionally one or more WebAdmin instances
(1 to n Application Server)
MS-SQL CLUSTER

Software Requirements

Operating system	Microsoft Windows Server 2016 or 2019
Database	Microsoft SQL Server 2016 or 2017
Application-Server	Microsoft Internet Information Services (IIS) JBoss Enterprise Application Platform (embedded)
Technology	JAVA 8

Advantages of Governikus MultiMessenger

Legal Certainty

GMM logs all process steps of incoming and outgoing communication, initiates all checks and generates clear processcards. This way, you can be sure that you have access to legally relevant information on all your communications at all times. In addition, you have the option of transferring all messages with all information directly to a long-term storage facility for long-term preservation of evidence. By supporting explicit access, you can be sure that you are communicating with citizens, customers and companies in the „right“ way.

Standardization

All interfaces are based on national and international standards, so that proprietary connection of systems can be dispensed with.

User Acceptance and Customer Satisfaction

Your employees can communicate easily and without background knowledge of communication systems, certificate checks, etc. from their preferred and familiar systems (e.g. eMail client). The access opening stored in the identity repository is just one point that your colleagues no longer need to worry about. External communication partners can communicate with you via their preferred channel.

Efficiency and Cost Optimization

Implementing an electronic mailroom enables you to serve all electronic delivery and receipt channels and integrate all your communications into established processes and systems without media discontinuity. Thanks to the flexible and simple handling of virtual mailboxes, preferred internal delivery systems can be adapted as needed without having to make adjustments or new installations in them.

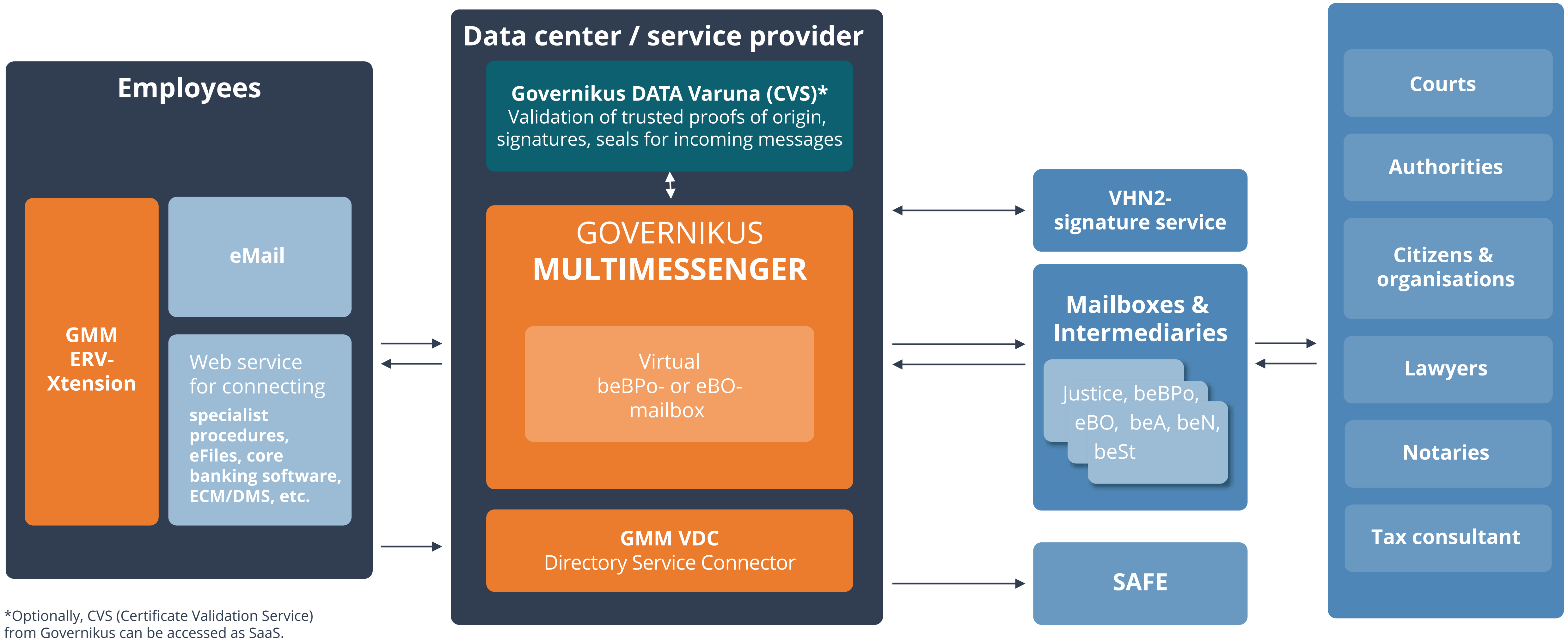
Future-Proofing / Investment Protection

New communication channels can be easily integrated into existing infrastructures and ensure provider neutrality, for example, in the event of changing or new requirements (e.g., when changing a De-Mail provider). GMM enables communication via different channels without the need to implement additional software. Your investment is protected by the assured maintenance and further development as a product of the IT Planning Council.

Multi-client capability

Due to its multi-client capability, GMM is ideally suited for operation in a data center. GMM enables any kind of billing mechanism and a client- and department-specific allocation of costs for the different communication channels.

Electronic Legal Transactions and GMM


Employees
GMM ERV-Xtension
eMail
Web service for connecting
specialist procedures, eFiles, core banking software, ECM/DMS, etc.
Data center / service provider
Governikus DATA Varuna (CVS)*
Validation of trusted proofs of origin, signatures, seals for incoming messages
GOVERNIKUS MULTIMESSENGER
Virtual beBPo- or eBO-mailbox
GMM VDC
Directory Service Connector
VHN2-signature service
Mailboxes & Intermediaries
Justice, beBPo, eBO, beA, beN, beSt
SAFE
Courts
Authorities
Citizens & organisations
Lawyers
Notaries
Tax consultant

*Optionally, CVS (Certificate Validation Service) from Governikus can be accessed as SaaS.

**eBOs CANNOT communicate with each other.

One example of a Governikus MultiMessenger deployment scenario is the special electronic public authority mailbox (beBPo) or the electronic citizens‘ and organizations‘ mailbox (eBO). Among other things, GMM is particularly suitable for the exchange of EGVP/OSCI messages and is approved by the judiciary as so-called ERV-SES (send and receive software) in the EGVP network. The supplementary Governikus products GMM ERV-Xtension, GMM VDC (Directory Service Connector) and SAFE-ID Manager make GMM a convenient solution for participating in electronic legal transactions.

For more information on complementary products, click here: https://www.governikus.de/en/loesungen/produkte/multimessenger/

We also offer the conversion of the beBPo for forwarding to an eMail client as a service. Information on this can also be found on our website: https://www.governikus.de/en/loesungen/produkte/bebpo-as-a-service/

About Governikus

We at Governikus have a vision: We stand up for digital sovereignty in a complex networked world. For more than 20 years, over 200 dedicated Governikus employees have been ensuring the protection of personal data with our secure and forward-looking IT solutions. We are convinced: Digitalization needs cryptography! Secure identities, confidential and legally secure communication as well as the handling of data worthy of protection to ensure authenticity and integrity are the focus here. As pioneers in eGovernment and eJustice, legal requirements, norms and standards are among the cornerstones of our developments and services. Know how that is needed and appreciated in the course of advancing digitalization in other industries, such as the healthcare market or the financial world. It is important for us to build on a consistent dialog with customers and partners. We support digitization projects with solutions that are used for shared basic infrastructures. With the products developed by Governikus for the IT Planning Council, the Governikus application, the GMM application and the DVDV, important standard modules are available to the public sector and the judiciary (as well as other administration-related institutions and organizations) at all federal levels. The federal government‘s AusweisApp2 for using the online ID card function is also being developed by us.

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

Branch Office Berlin
Universitätsstraße 2
10117 Berlin, Germany

Branch Office Köln
Herwarthstraße 1
50672 Köln, Germany

Branch Office Erfurt
Johannesstr. 162
99084 Erfurt, Germany

Branch Office Kempten
Klostersteige 17
87435 Kempten (Allgäu)

Follow us on social media:

in @governikus

X @governikus

▶ @governikus

Status 04/2023

governikus.de