

Service certificate

STACKIT MailOut

Version and start of validity

Version 1.0	Valid from 2026-09-18
-------------	-----------------------

Service certificate | STACKIT MailOut

Service name

STACKIT MailOut

High level service description

STACKIT MailOut is an email delivery service that may be used exclusively for the automated, outbound sending of emails. The service does not include the receipt of incoming emails, reply routing, or bidirectional communication functionality. It is intended for sending transactional emails (such as user registrations, login notifications, and order confirmations) as well as marketing and campaign emails. In all cases, delivery is exclusively automated and one-way.

Key Features

- Scalable, highly available delivery infrastructure with high-reputation IP pools for maximum delivery rates and reliability.
- Enables the scalable sending of large volumes of emails (transactional and marketing/campaign emails).
- Optionally, customers can use a dedicated IP address for sending emails.
- Customers can set up and use their existing domains as sending domains. MailOut does not provide email mailboxes, email addresses, or email accounts for end users. The use of customer-owned domains serves exclusively to identify outgoing sending domains.
- Compliance with common email authentication standards (SPF, DKIM, DMARC) to be classified as a trusted sender with a high sending reputation and thus ensure high delivery rates.
- Support for advanced security features such as MTA STS / DANE / DNSSEC.
- An SMTP relay is available for easy integration with existing servers or systems.
- Automated handling of emails that cannot be delivered (hard and soft bounces) and spam reports (complaints).

Service Plans

-

Metrics

Billing is usage-based, calculated per email sent by the Customer and per kilobyte (KB), based on the following metrics. The data volume is continuously tallied and calculated per partial kilobyte:

- Message volume (number of email messages)
- Message size (in kilobytes)

SLA Specifics

The service is considered available when the central API or the SMTP relay successfully responds to email submission requests.

STACKIT assumes no responsibility for the successful delivery, acceptance, storage, display, or acknowledgment of the email by the end recipient, nor for its processing by receiving mail servers. The availability of the service does not depend on whether an email is successfully delivered, accepted, or processed outside the STACKIT infrastructure. To the extent that MailOut transfers emails to downstream mail servers, this is done via generally available Internet and email infrastructures that are not under the sole control of STACKIT.

Backup

- Emails are not backed up.
- The MailOut environment and its configuration are backed up automatically according to a schedule specified by STACKIT in line with the STACKIT Cloud general service description. This schedule cannot be changed by the Customer.

Additional terms

- The Customer is responsible for configuring MailOut.
- The Customer is responsible for and liable for all emails sent from their project.
- In particular, the Customer is responsible for the content, recipients, reason for sending, legal basis, consents, opt-out options, recipient lists, sender information, and compliance with applicable data protection, e-privacy, competition, and digital services regulations.
- STACKIT places the highest priority on security, integrity, and compliance with the guidelines established by STACKIT. The STACKIT MailOut service may be used exclusively for the automated, one-way sending of emails by the Customer. This includes transactional emails as well as marketing, newsletter, and campaign emails. The use of MailOut as an interpersonal communication service - in particular as a substitute for an email client, as a mailbox service, or for the exchange of messages between individuals - is not permitted. The sending of unsolicited promotional emails (spam), phishing emails, and all malicious emails and illegal content is expressly prohibited.
- Transactional emails are emails triggered automatically by an event in the Customer's systems or applications that are directly related to the use of a product, service, user account, or transaction by the Customer (e.g., order confirmations, registration links, password resets, system notifications). For the purposes of this Service Specification, marketing emails are emails sent automatically to recipient lists for promotional or informational purposes (e.g., newsletters, product announcements, campaigns). Marketing emails are also sent exclusively one-way and automatically via MailOut. A two-way exchange of messages is not possible through the service.

- STACKIT is entitled to temporarily or permanently block, limit, or suspend the sending of individual emails, sending domains, service accounts, IP addresses, or projects if there are concrete indications of spam, phishing, malware, illegal content, reputational risks, security risks, or other misuse.
- The Customer is solely responsible for complying with any obligations under telecommunications law if the Customer uses MailOut or integrates it into their own products in a manner that makes them a provider of telecommunications services as defined by the German Telecommunications Act (TKG).
- The Customer is responsible for maintaining the Suppression List (list of suppressed recipient addresses). STACKIT automatically adds recipient addresses to the Suppression List in the event of hard bounces. The Customer may manually add or remove entries. The Customer is responsible under data protection law for the personal data (email addresses) stored on the Suppression List.

Annex | Exportability

(Online Register)

Data type	Description	Exportable (Yes/No)	Format	Additional notes
Customer data (database content)	Data stored by the customer in the database (if available) or within the product/service	No	-	The SMTP relay stores the email or data to be sent only until it is successfully delivered to the recipient's mail server; the data is then automatically deleted. Email content is not stored permanently. Sending metadata (subject, IP addresses, sender, recipient, message IDs, email size, attachment size, SMTP status codes) is retained in STACKIT logs for 14 days and made available to the Customer in the portal as "Message Tracking." After 14 days, the metadata is automatically deleted.
User accounts & permissions	Information about users and their permissions	Yes	JSON	The service accounts for SMTP authentication can be listed and saved via the API.
System metrics (instances / resources in use)	Performance data of the instance / resource in use (e.g., CPU usage, memory usage)	No. Company confidential STACKIT.	-	-
	Sizes and capacities <i>Capacities of the available resources / instances</i>	Yes	JSON	Metrics are available for tracking the usage of all key quotas.
System properties (instances / resources in use)	Versions and information necessary to check compatibility	No	-	STACKIT MailOut does not use publicly available versioning

Product- / service-related data (product properties)	Configuration data and source code	No. Company Confidential STACKIT	-	-
	<i>Configuration of IT-systems / rudimentary IT, settings, customizing, IP's, VLAN, interfaces, software code, scripts</i>			
	Log data (non personalized and personalized)	No	-	STACKIT Internal. Technical logs (system status, events) do not contain any personal data. Bounce/complaint data and delivery metadata are subject to a 14-day retention period.
	<i>System-status, technical-events, etc.</i>			
	Log data (non personalized and personalized)	Yes	JSON	STACKIT Audit Log
	<i>Login/logout of user, user activities</i>			