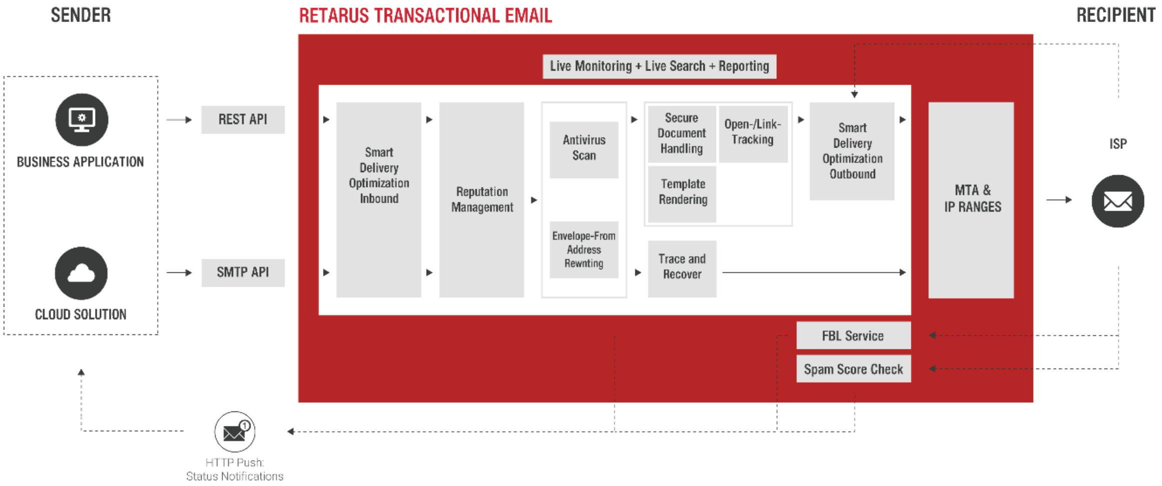
Service Description and Duties of Cooperation
Retarus Transactional Email

Using **Retarus Transactional Email**, large volumes of emails can be sent from business application directly, without burdening the customer's own email infrastructure. To this end, the customer's infrastructure will be connected to the Retarus Enterprise Cloud via standard interfaces. The data is processed in Retarus' own data centers.

System Architecture of Retarus Transactional Email



INTERFACES	REST (V2)	SMTP
Max. Volume Sent per Hour	Scalable as required	Scalable as required
Smart Delivery Optimization	✓	✓
Status Information for Each Email	API-Callback (Webhooks)	API-Callback (Webhooks)
Email Reporting (CSV)	✓	✓
Smart Network Data Services Reporting*	Upon request	Upon request
Reputation Management	• Dedicated IP (optional) • Blacklist-Monitoring • Live monitoring • SPF/DKIM • Suppression list • Registered Sender Domain • Feedback-Loop-Service* • CSA certified (EU, CH) • IPv6/IPv4 support	• Dedicated IP (optional) • Blacklist monitoring • Live monitoring • SPF/DKIM • Suppression list • Registered Sender Domain • Feedback-Loop-Service • CSA certified (EU, CH) • IPv6/IPv4 support
List Unsubscribe Header Support	✓	✓
Multi-Client Capability (Multi Domain Configuration)	✓	✓
IP-Whitelisting	✓	✓
Encrypted Connection to the Retarus System	✓	✓
Technical Requirements	HTTPS API client (job) and receiving web service (status)	Application with SMTP support (job) and receiving web service (status)
Open Tracking	✓	-
Link Tracking	✓	-
Envelope From Address Rewriting	✓	✓
Bounce and Response Manager	✓	✓
Secure Document Handling	✓	-
Template rendering	✓	-
Trace and Recover	-	✓
Spam Score Check	✓	✓
EAS Live Monitoring	✓	✓
EAS Live Search	✓	✓
EAS Reporting	✓	✓
Max. Mail Size	20 MB	20 MB

* These functionalities require using IPv4 addresses.

Basic Configuration

The basic configuration includes access data, or a registered authentication IP for an API end point or an SMTP server in a Retarus data center. Communication will take place using a secure connection via HTTPS and/or SMTP Auth Basic via eTLS. The setup includes a sender domain/IPv6 address, default job parameter, IP Routing, SPF record and DKIM signature. The account will be activated after complete setup of the requested packages and an interface description will be provided.

*Clarification on IPv6 address: The use of the following functionalities with the services require using IPv4 addresses:

- Smart Network Data Services reporting
- Feedback-Loop-Service
- CSA-certified IP areas (Certified Senders Alliance)

Dedicated IP

One or more sender domains will be allocated a dedicated IP address. By doing so, e. g. the email traffic from various applications, parents or subsidiaries can be differentiated. Using Dedicated IP is recommended for volumes of ≥ 1,000,000 emails monthly. Given that the Transactional Email Service is generally connected to a group of data centers (active/active), the use of Dedicated IP requires at least two dedicated IP addresses. Once the dedicated IP addresses are set up, Retarus will provide IPv4 addresses for Customer’s use for the duration of the contract term. These will be integrated into Retarus' blacklist monitoring system. Retarus reserves the right to exchange the IP address at any time.

Enforced TLS

During the basic configuration of the Service, it will be determined at the sending domain level, whether a hybrid encryption protocol is to be used for every email sent. Thus, the system attempts to establish an encrypted connection as soon as the Customer sends emails via the specified domain (enforced TLS). If an encrypted connection is declined on the recipient's side, the sending process will be cancelled.

Envelope From Address Rewriting

Optionally, Retarus offers Envelope From Address Rewriting for outbound emails in order to re-direct potential replies to a dedicated inbox. Rewriting of addresses is especially useful if, for example, corporate policies do not allow emails to be sent into the open Internet via the company's own domain.

Account / Access Token

An account is defined as an authentication unit (definition of API username/password, etc.) and is related to a specific data center, API access point. Multiple domains can be managed under each account. You can also manage the same domain under multiple accounts.

Smart Delivery Optimization

Retarus uses smart send and receive control of emails based on the sending domain. Smart Delivery Optimization automatically adapts the Customer's sending behavior to the responses of individual ISPs and/or ESPs in order to keep the message throughput high for ISPs and/or ESPs. In exceptional cases, optimized transmission management can lead to a reduction in the agreed processing capacity.

Status Information via API Callback (Webhook)

Retarus offers status information via API Callback (Webhook). The customer will be informed of newly-created events, e.g., delivery status, reasons for undeliverability, blocking of emails to recipients in the Suppression List, and information about open and link tracking. These status information types can be automatically integrated into business processes and applications via HTTP POST, e.g., to maintain master data (database hygiene) or support the reputation of the customer's own domains.

Retarus EAS – Live Monitoring

Retarus offers Live Monitoring in its EAS Portal, through which emails can be tracked in real time. Using this solution, the customer can recognize trend developments in the areas of delivery, soft/hard bounces and dropped messages, and initiate counter measures accordingly.

Retarus EAS – Live Search

Retarus EAS Live Search provides a transparent overview over sent emails. EAS Live Search enables Customer to search for outbound emails based on time periods, message IDs, senders and recipients, and to obtain detailed status information of the past 45 days.

Retarus EAS – Reporting

Retarus EAS Reporting provides a transparent overview of emails sent in the past 45 days, downloadable as CSV or Excel (XLSX) file.

Observability Metrics

The Observability Metrics feature provides a dedicated federation endpoint to retrieve metrics data in Prometheus Exposition. Retarus provides access to data from the Transactional Email backend, allowing fast and seamless integration of these insights directly into your existing systems and workflows, using familiar tools and applications in customer environment.

Email Reporting (CSV)

Via the EAS, Retarus provides a daily transmission report in CSV format available for retrieval by Customer for a period of 180 days. These reports only include transactions with a final status. Transactions that are still being processed are not listed. The report can be accessed as several file parts or compressed (e.g. as a ZIP file).

Please note: Creating a CSV report requires temporary data storage for service provision purposes. The data stored includes information about message processing as well as personal data, such as senders' and recipients' email addresses, but no content data.

Retarus Spam Score Check

The likelihood of messages being categorized as spam depends on several factors. Unusual HTML formatting or table structures, excessive numbers of links or dubious wording used in the subject line or the text body can trigger spam warnings. The purchase of the optional Retarus Spam Score Check service enables Customer to check their emails for the probability of being categorized as spam – before sending. The SpamScore is returned via an automated process which transmits the determined information from Retarus via email to the reply-to address provided by Customer, or via API Callback to Customer's available web service. After transmission, all related information is deleted; no data will be stored.

Open and Link Tracking (optional CNAME)

Open Tracking allows Customer to determine the opening rate of emails, while Link Tracking enables Customer to track the opening rate of links contained in emails. The respective email body and/or the link will be modified so that the messages can be analyzed. To reduce the potential of as spam classification, Retarus recommends the purchase of the CNAME option, which allows Customer to use one of their own (sub)domains. In this case, the Customer associates an A Record of the respective (sub)domain with a Retarus server address.

AntiVirus Multiscan

Retarus checks messages for viruses during the sending process, using two virus scanners from different Retarus providers. Retarus will use provider updates or new releases as made available. The Customer can pre-define, whether only attachments and/or the body of an email are to be checked for malware. If a virus is detected, Retarus deletes the infected email. Status information for infected emails will be provided to the Customer via API Callback (Webhook).

Secure Document Handling

File attachments in emails to be sent can be encrypted with Secure Document Handling. Attachments will be automatically packed in a password-protected ZIP archive in the Retarus System before sending. The passwords will be provided to the recipients in separate emails. In order to provide the highest possible protection to recipients, this feature is only available in connection with Retarus' Outbound AntiVirus MultiScan service.

Trace and Recover

This feature marks emails sent via an SMTP connection as Trace & Recover messages. Messages marked for Trace & Recover are stored in short-term storage for a period of 45 days and can be found during this period using the Retarus EAS Live Search function. For marked messages, a preview of the first 1,000 characters is available. Before a message can be re-sent, if required, only the initial recipient can be edited.

The additional Trace & Recover function requires AntiVirus MultiScan and is activated by Retarus for a technical account to be determined by the customer. Trace & Recover cannot be used in connection with Envelope-From Address Rewriting (outbound).

Processing Capacity

Processing capacities are calculated in accordance with the basic configuration of Transactional Email assuming an email size of 200 kilobytes and including Open and Link Tracking for a one-hour period.
A contractually agreed processing capacity on an hourly basis requires an even distribution of transmission requests at Retarus over the course of an hour by the Customer as outlined in the example below. To provide the agreed throughput, Retarus checks the distribution in 5-minute intervals.
Due to possible send peaks, the actual processing capacity may be 1.25 times the agreed processing capacity. In the case of additional features or larger emails, the bandwidth may decrease (e. g. for emails larger than 200 KB). Deviations in processing capacity may occur from time to time. A review of Customer's individual requirements by Retarus is essential before processing capacity can be increased.

Example: Processing Capacity

In the following example, the contractually-agreed processing capacity is 150,000 emails/hour:

(150,000 emails/hour) / (12 x interval*/hour) = 12,500 emails/interval*

The maximum extension for send peaks of 25% can increase the thoughput to a maximum of 15,625 emails/interval*.

*One interval is 5 minutes.

IP-Whitelisting

With the Retarus IP-Whitelisting feature Customers can improve their 'permitted transmission' security. Customers expressly define which applications in their network are allowed to use the Transactional Email Service and which are not.

Feedback Loops

Retarus communicates with different Internet service providers ("ISP")via complaint agreements. Complaint information will be reported back to Retarus by these ISPs in the form of feedback loops (ARF).

Feedback loops are a mechanism provided by the ISP to inform senders (here Retarus) when their messages are classified as unwanted. 'Unwanted' refers to your message being classified as spam by the email recipient (e.g. click on 'This is spam' in their own inbox).

The complaint feedback is carried out in an automated process, in which the complaint information transmitted is read out and fed back by Retarus – via email to Customer's reply-to email address or via API Callback to Customer's available web service. After transmission, all related information is deleted; no data will be stored.

Billing

Emails are charged per unit, with one unit being 200 kilobytes. Emails exceeding 200 kilobytes will be split into several units for billing purposes.

Example: An email is 2,403 kilobytes (approx. 2.4 MB): this equals 13 billing units.

Emails are invoiced (identifier: email ID) regardless of successful delivery (e.g. if blocked or bounced).

Duties of Cooperation

The customer is aware that successful use of Retarus services and the quality of the services provided depends considerably on the customer's cooperation. The customer, thus, will return the filled-in Implementation Sheet, which was provided to them upon conclusion of the contract, within five (5) working days, will adhere especially to the duties of cooperation set out in this document and agrees that Retarus may take technical measures beneficial for securing stable service provision and the parties' ISP reputation. To this end, Retarus is expressly permitted to discard specific email orders, restrict the volume or, in extreme cases, ban access. Should efforts and/or cost arise from non-compliance with duties of cooperation, these are to be covered by the customer.

The Customer undertakes to solely send emails to recipients who, according to the applicable regulatory and legal framework, have given their express consent (opt-in) to receive such emails, unless other legally recognized permission exists. Customer shall comply with notification requirements, privacy statements e.g. in the context of Open or Link Tracking - or otherwise, if applicable – in accordance with applicable laws and regulations.

Email Design

Each email sent must contain easily identifiable legal details that comply with the applicable statutory requirements.

Additionally, the following applies to emails with advertising/promotional/marketing content:

- The initiator of such emails must be clearly recognizable.
- In each email, the recipient must be made aware of the option to unsubscribe or opt out from receiving emails at any time. In general, opting out/unsubscribing from emails must be easily doable for the recipient, i.e. without entering access data (e.g. login or password).
- Neither the sender nor the commercial nature of the email may be disguised or concealed in the header and/or subject line of the email. An email is considered disguised or concealed if the header and subject line are intentionally designed in such a way that the recipient receives no or merely misleading information as to the sender's actual identity or the commercial nature of the message before reading the content.

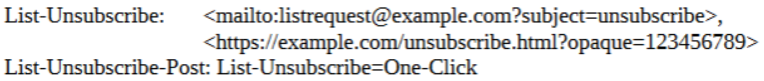
Technical Configuration

- Sender addresses must be registered and be included in the service administration. The sender address must be able to receive emails (valid DNS MX record). The sender domain must also have a valid DNS A-Record. Role-based sender addresses (e.g. abuse@ or postmaster@) are not permitted.
- The Customer must immediately delete email addresses from the respective mailing lists if non-existence of the address is discovered upon transmission, and at the latest if three hard bounces have occurred. The total hard bounce rate per ISP shall generally not exceed 1.0%. Role-based recipient addresses (e.g. postmaster@, abuse@) will be rejected/discarded.
- The Customer must delete email addresses from the respective mailing lists if the recipient categorizes an email as spam and reports this (complaint) or revokes consent to receiving emails.

- For the 'MAIL FROM' address specified in the SMTP communication between email servers, an SPF-From Record must be entered, thereby allowing an SPF test to be carried out on the recipient side. The SPF Record must end in "-all" or "~all". In case the necessary entries are not made on the Customer's side within ten (10) business days, the re-verification efforts and expenses will be charged in accordance with Retarus' agreed hourly rates.
- The use of the DKIM (DomainKeys Identified Mail) method is mandatory. For each sender domain registered with Retarus on behalf of the Customer, the Customer must store a corresponding DKIM key in their DNS. If Customer fails to make the necessary entries within ten (10) business days, the reverification will be billed in accordance with Retarus' agreed hourly rates.
- A 'List-unsubscribe'-header or a 'List-help'-header (see RFC 2369) must be included in every email. The 'List unsubscribe' header is required for list-based mailings, and has to be inserted with a 'POST HTTPS'-link including a 'One-click unsubscribe' feature (RFC 8058). The link provided must trigger a direct one-click unsubscription at least at list level. The sender may send unsubscribe confirmation emails. In non-list-based mailings, the 'List-help' header shall be set as an alternative to the 'List-unsubscribe' header. The 'List help' header shall include at least one 'mail-to' address or a HTTPS link. HTTP links are not permitted. Both the use of the "mailto" address and the HTTPS link must enable the recipient to receive information about the reason why the email was sent to them and why unsubscribing at the list level is not possible.

- Using the „list-unsubscribe-Post"-Header requires a valid URL address which can receive and process such POST requests.

  Example:



```
List-Unsubscribe:      <mailto:listrequest@example.com?subject=unsubscribe>,
                       <https://example.com/unsubscribe.html?opaque=123456789>
List-Unsubscribe-Post: List-Unsubscribe=One-Click
```

- Exceptions to these obligations may apply if it is not required or possible to unsubscribe as described above due to the configuration of the Service and the associated transmission of automated emails.
- The Customer must set up an abuse email address for the reporting of the abuse of email addresses for the addressees of the emails and monitor it. The abuse email address can be configured for example as abuse@domain.
- The delivery of emails to the Retarus Transactional Email service must take place via Transport Layer Security (TLS – opportunistic/enforced) from the customer, according to the current state of the technic. Retarus uses for sending emails to the addressee Transport Layer Security (TLS) while using CSA IP-addresses.
- Retarus is Certified Senders Alliance ("CSA") certified. The cooperation duties described herein reflect the current CSA requirements. The CSA reserves the right to adapt their requirements at any time, in which case Retarus will notify Customer accordingly. Customer agrees to comply with any such changes.