sinch

Sinch E-Mail 365 Internal Document: Frequently Asked Questions

Version 10 – Feb 2022

sinch.com

Revision History

Version	Date	Description
1.0	12/24/2019	First draft
2.0	1/2/2020	Updated question on Blacklist and added SMTP interface question
3.0	1/20/2020	Data retention policy and location of Email Server data centres
4.0	1/24/2020	Question on Whitelists, Spam labelling, Gmail and yahoo FBL, Email 365 Marketing roadmap
5.0	2/29/2020	Synchronous and Asynchronous bounces and SMTP
6.0	03/03/2020	Updated Retry policy details
7.0	04/05/2020	Recall emails, encryption support and unsubscribe options
8.0	05/19/2020	Information on SPF and DKIM
9.0	07/10/2020	Information on DMARC and on hosting platform for E-Mail service
10.0	23/02/2022	Updated the information in FAQ questions, changed the template of the doc

Table of Contents

Audience

This document is intended for internal use only by E-Mail 365. This document is not to be shared with customers, press or analysts.

Purpose

The purpose of this document is to provide you with a selection of the most frequently asked questions and answers about our product Sinch E-Mail 365. The document has been created to ensure you are equipped with the Sinch communication guideline.

1.1 What is Sinch E-mail 365

Sinch E-Mail 365 provides an enhanced JavaScript Object Notation (JSON) interface with easy-to-use RESTful calls and allows enterprises to deliver emails using a single API
It enables enterprises to confidently integrate e-mail with their existing applications in a single notification and engagement strategy.

Pitch Deck: Work in Progress, will share by end of Q2. Please get in touch with the product team

Solution Brief: Work in Progress, will share by end of Q2. Please get in touch with the product team

1.2 Is this an existing product?

Yes. Sinch E-Mail 365 is an existing product (previously known as Intelligent Notification 365, Email or IN 365) that has been rebranded to Sinch E-Mail 365

1.3 How do we pitch it?

Working on a pitch deck, will share the updated one by end of Q2. Please get in touch with the product and business team for the details

1.4 How do we price it?

Working on a new pricing, will share the updated one by end of Q2. Please get in touch with the product and business team for the details

1.5 Does Sinch E-Mail 365 support 2-way communication

Sinch Email 365 API supports one way communication. Customer cannot use the API to receive emails from users, also we do not provide mailboxes / inboxes for incoming emails.
The replyTo email address set during the API request should point to an existing mail boxes. Users can reply to this replyTo email address and incoming emails can be received by customers on their existing mailboxes. Incoming emails do now pass through our infrastructure.

1.6 Is Sinch E-Mail 365 GDPR compliant?

Sinch E-Mail 365 is fully compliant with GDPR requirements

1.7 Are API requests secure?

Sinch E-Mail 365 API uses HTTPS (secure HTTP). All API requests are encrypted since they are sent over HTTPS that uses TLS encryption protocol

1.8 What does the email service use for sender authentication?

Both SPF (Sender Policy Framework) and DKIM (Domain Key Identified Mail) are used for authenticated email delivery.

- DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic (public private keys) authentication. Identification of an email association with a trusted domain enhances deliverability.
- Sender Policy Framework (SPF) is a simple email validation system designed to detect email spoofing by providing a mechanism to allow receiving mail

exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrator.

1.9 What is the level of throughput supported?

We are constantly reviewing customer requirements and accordingly increasing our throughput, through capacity increase & platform optimization, while adding better monitoring mechanisms as well.

Currently the throughput is supported by 2 instances of Email Servers, whose information is given below:

The throughout supported on 1st instance of Email Server

1. EU Datacentre: 3M emails / hour
2. US Datacentre: 1.5M emails / hour

The throughout supported on 2nd instance of the Email Server is

1. EU Datacentre: 1M emails / hour

This is a shared throughput on the data centre that is available to all customers, we do not guarantee throughput for customers.

.

1.10 Where is the Sinch E-Mail 365 datacentre located?

Sinch E-Mail 365 datacentre is in EU Ireland. We have one datacentre in EU and our one instance has 2 mail servers, one located in EU datacentre and one in US datacentre

1.11 Where is the instance 1 (Email Server) Datacenters located?

- US Data center is located in Secaucus
- EU Data center is located in Frankfurt

1.12 Can you explain the workflow for Sinch E-Mail 365?

Please refer to the snapshot given below in 1.54

1.13 What features are supported by the Sinch e-mail 365 API?

Core features supported by Sinch Intelligent Notification 365, email service includes:

- Domain and user validations
- DKIM & SPF based deliverability
- Support for multiple senders per sub domain
- “Reply to” capability
- Support for custom “from” tags
- Soft and hard bounce status reporting
- Reputation management support
- “Reply to” tracking using a dedicated MX record

1.14 Can the API be used to send email to multiple recipients?

The API supports multiple recipients. It can easily be handled by passing multiple recipients in the parameter list for delivering common message to bulk recipients

1.15 How are these requests with multiple recipients handled?

Sinch E-Mail 365 delivers each notification as a separate request to report on the request status individually.

1.16 Can we provide test accounts for customer who would like to test the API first?

Yes, we can have them onboarded on our Sinch test domain. You will need to complete the provisioning form and create a CRM request for a test account on E-Mail 365.

1.17 Are attachments supported?

We are currently not allowing customers to send attachments through our existing environment because the bigger attachment emails and higher volume slow down all our marketing customers. In order to support bigger attachment sizes, we will need to build a new environment (dedicated for emails with attachments) and there might be an additional cost to this for the customer.
Approval is needed for access to sending smaller sized attachments. Currently this is being handled on a case-by-case basis

1.18 Is the Intelligent Decision 365 a part of this service?

No, Intelligent Decision 365 is not a part of (or included in) this service

1.19 What other channels are supported?

Only Email is supported through the Sinch E-Mail 365 API

1.20 How to get email metrics?

Currently we don't track open, click and other metrices for the email sent via E-Mail 365. We only track delivered and bounced email ids

We can provide excel reports through BO, but these are only for customers directly integrating with the E-Mail 365 API. We are also building a reporting module for email metrics through the Unified Messaging platform that may be available around Q3 2022

1.21 Can a customer use existing email for reply-To Address instead of creating new reply address?

Yes, any address can be used as long it's a valid and real email address. Additionally, noreply@ and a different domain, although not ideal but it is possible to use.

1.22 What are the benefits of using a new subdomain for marketing emails over the existing main domain?

The benefits of using a sub domain (for marketing) e.g., marketing.customdomain.com is that

- ISPs would tend to recognize the emails coming from this domain as being Marketing type of emails and therefore more likely to accept them (as long as other aspects are adhered to e.g. good content, clean contact lists etc).
- The next benefit is if there are Sending Reputational issues then this will not have a major impact on the main domain, which could in theory effect their ability to send emails on that domain.

1.23 When do we receive bounce information?

Depends on the ISP. In most cases bounce statuses can appear within minutes of delivery, but in some cases, it can take hours

1.24 When will a campaign have the final number of Soft Bounces?

Usually before 24 hours, but can take around 48 hours after all the retries are completed

1.25 How often do you retry to send the message?

All soft bounces are retried in a 48-hour window

- The first two retries after 30 minutes.
- Thereafter one retries after every ~ 65 minutes.
- After 48 hours it ends with final status if there was no successful delivery possible.
- Total number of retries should be around 48 (including the final status)

1.26 What are the best practices and recommendations for improving deliverability?

Please refer to the deliverability best practices guide

1.27 What are the requirements for a customer?

The customer needs to setup DKIM, SPF and MX records on their DNS.

- Sinch provisioning team will send over the DKIM and SPF
- The customer needs configure these in their DNS and the MX record (MX record is not provided by Email 365, the customer has to use their own).

    - The customer needs to specify their mail server in the MX record that is responsible for accepting email addresses on behalf of their sub-domain and this MX record is added to their DNS
- Our team will validate these and advise

Note: The update of DNS settings/records are the responsibility of the Customer and they should seek advice from their DNS Managers (IT or otherwise) to ensure these are amended correctly

1.28 Are there any additional requirements for customers directly integrating with the Sinch E-Mail API (non-marketing customers)?

Additionally for customers that are directly integrating with the API, they need to make sure that their applicate is capable of managing Sender Reputation such as:

- Content Validation method available (possibly via external tool/product)
- Contact List Double Opt-in process in place and / or email address validation (possibly Never Bounce)
- Method to remove Hard Bounces, due to bad email address / Complaints
- Method to remove List Unsubscribe contacts
- Soft Bounce Policy (removal of contacts which have soft bounced after 3 Campaign attempts)
- A way to manage target lists (not sure if this customer is sending Marketing types of emails) to ensure relevance of content

1.29 What is MX record?

An MX record is a publicly available address for an email recipients mail server. When someone, for example:mtest@test.com sends an email to abc@xyz.com, the sender's mail transfer agent looks up the available MX record at public DNS registry of xyz.com to determine where to deliver emails.

1.30 Why is MX record mandatory?

MX record is mandatory to avoid failing anti-virus checkers against the registered domain/sub domain for this service. The MX record is also needed for “reply” tracking. The “reply to” address allows a recipient to respond back to an email. When a marketing / transactional email is replied to, the mail transfer agent looks up DNS entries to determine the MX record of the recipient’s mail server.

1.31 What should the customer configure as A and MX?

- **A** – This should already exist for the Sending Domain / Sub Domain and is not provided by Sinch. As an example, an A Record is used to point a logical domain name, to the IP address of domain names hosting server, eg: "74.125.224.147".

- **MX** – This should reflect the receiving email server address for the domain. This is not provided by Sinch and should reflect where emails are received at the Corporate Domain / Sub Domain (similar to providing a Postal Code or PO Box# where letters would be received, if being returned. This is required to prevent spam agents rejecting the message because of no return address being identified)

1.32 How does Amazon SES allow quicker warmup, compared to our warmup schedule?

The main reason is that Amazon SES infrastructure uses Shared IP’s for the majority of users and involves a mixture of email types e.g. transactional, B2B & marketing etc. This allows their users to warm up faster because they have a much broader reach in terms of volume and email types to the main ISP’s. If a customer used our shared IP’ s, then the warm-up plan is faster (as per the Template), but not necessarily as fast as Amazon SES.

The Warm-Up Guidance is based on our experience with other marketing or blast email customers. The rate of increase can be accelerated later in the plan, based on

the results. The results are dependent on content, clean contact lists and overall sender reputation".

1.33 If a customer wants to use an existing domain, do they still have to go through warmup?

Yes, because this existing domain needs to be warmed-up to send emails from our IPs

1.34 Do we have a tool or solution that can validate email addresses?

No, we don't such a tool or solution. We can recommend some 3rd party tools/products which are available.

1.35 How can a customer monitor deliverability or reputation?

This can be done via 2 key mechanisms

- Using bounce reports: Both Soft and Hard bounces are reported (as long as the recipient SMTP server provides the status).
- Using sender score reports: Sender scores are industry standard for reporting on a sending domain or IP address' acceptance within the ISP community. This can be monitored by Return Path (a 3rd Party)

1.36 For select FROM: email accounts can we change the DISPLAY name on the emails? Example: howzit@mail.incredible.co.za show up as (Incredible Marketing)?

Our API offers “senderName” parameter as custom from tag which allows a unique name to be tagged to a “sender address”. For example, if we set up the “senderName” tag as Mark Jones, the sender address will then show as Mark Jones support@abc.customer.com

1.37 What happens if an IP gets blocked? Are there any costs involved if the single IP was blocked and a resend is triggered? What are the timelines for unblocking?

Normally the customer has to follow up for delisting the IP. We don’t charge customers for the support we at Service Desk provide for requesting the delisting of an IP from blacklisting. If a customer asks us to assist them with an un-list, then this is part of our standard operating procedure to assist them. This is in addition to customers who often contact the “reputation block” service themselves for the blacklist removal.

Every blacklist is different and each one has their own listing criteria and severity for the blacklist (the level of offence). After submitting a request for removal of the IP from the blacklist it normally takes 24-48 for delisting the IP. However, in some severe cases the customer may be asked to submit a root cause analysis and corrective action by the blacklist. In this case it may take a few days.

Please do understand that there is no guaranteed method or timeline of removing the IP blacklisting as the ownership is with a third-party provider who we have no relationship with and they have no obligation also to remove it

1.38 What is Smart Delivery Optimization - Outbound?

The Smart Delivery optimization – outbound feature can adjust the outbound sending rate by automatically adapting the customer's transmission behaviour to receiving and throttling behaviour of the respective ISP's. This will help the customer to avoid soft bounces from ISP’s and to strive for a higher deliverability of messages

This reacts on key words from the ISPs SMTP message reply. If any of the key words match, the email delivery is throttled

1.39 What are the limitations of SDO outbound?

In general, SDO is reacting on ISP feedback (SMTP reply). If there is a clear response from the ISP that we currently sending too much traffic, then SDO will throttle the transmission rate. If such response / feedback is missing then SDO will not act

SDO does not use ISP/ESP specific rules nor will such be used across the customers. The sending rate will not be limited in advance due to any ISP existing rules. There are no fixed rules set up for each ISP, which means SDO reacts dynamically based on the ISP feedback (SMTP reply)

SDO only works in case of soft bounces. If an ISP returns feedback as a 5xx error (in case of QQ) which may result immediately in a hard bounce (other ISPs normally return a soft bounce), then in that case, SDO will not take effect.

1.40 Do we support an SMTP interface?

We do provide support for an SMTP interface. The SMTP interface is a direct access to an SMTP server in the Email infrastructure. When provisioned the customer will be given credentials (account name and password) with a URL to connect to the SMTP adapter
Every account will have a one-time setup fee and a monthly fee. This is in additional to the per email price and domain set up fee which is still applicable.

1.41 Do we store email content? What is the email retention policy?

We do not store any email content at any point

1.42 What is the data retention policy?

We do not store any email content at any point. We only store email status and metadata for one week on the E-Mail 365 platform and after that for 2 years in cold storage / DB after which they are also deleted

The status and metadata fields are -
"account":
"notificationId":
"statusCode":
"statusText":
"timestamp": ",
"recipient":
"channelStatusCode":
"channelStatusText":
"campaignId":

1.43 Should customers sign up on ISP whitelists?

Signing up on ISP whitelists is not recommended by us. Being whitelisted by an ISP may help in quickly unblocking of IP address in case it is blocked for no reason. Besides, this there isn't much advantage in being whitelisted by ISPs, in fact such customers are held to a higher standard and if they don't follow good sending practices then they are blacklisted immediately.

If the customer follows good email sending practices such as:

- delist inactive users,
- remove users that opt-out,
- bounce management
- remove spam complaints

This will improve email deliverability. Customers that maintain good email delivery standards practices do not need to be whitelisted and get the email deliverability that they deserve.

Whitelisting through an ISP does not increase email deliverability because customers are still expected to follow all the best practices of sending bulk email

Shared IPs should not be whitelisted through ISPs

1.44 If an email goes to the spam folder after being flagged by the ISP, will the E-Mail 365 platform receive a complaint notification?

No, if the email hits Spam folder, then this is the end user email provider protecting the customer so they can review and decide if they want to "complain" and there won't be a "complaint" notification. The "complaint" notification is sent when the user interacts in some way to mark an email as spam, move email to spam folder or to block a sender

1.45 What is the roadmap for E-Mail 365?

Currently the roadmap is work in progress, will update on the roadmap by end of Q2'2022. For more details please get in touch with the Product and Business team

1.46 What are CX services? Do we recommend these services?

CX Services are expert consulting services that guide customers using recommended best practices around email marketing. We recommend these services for customers who need guidance and help during
We have success stories through implementation with Asian Paints, Barilla and Coty

1.47 What are synchronous and asynchronous bounces? Why in some cases a bounce may occur after an email is accepted by the mailbox?

Synchronous bounces: These are the majority of bounces. When an email is sent it starts an SMTP connection with the recipient mail server. In most cases, a recipient server will either accept or reject an email as it comes in. In those cases it will look at the email, and issue a code 250, which means the message is accepted. If it's bounce, it will issue a code in the 400's or 500's and this is sent back to the sending server within the open SMTP connection. As a result, we are able to receive these bounces back on our platform

Asynchronous bounces: In a few cases an asynchronous bounces may occur after the SMTP connection is closed, which means that the recipient server accepts the senders' email first and returns a 250 OK delivered response Then it does some

evaluation on the message, decides it's undeliverable for whichever reason and sends back an NDR bounce. These bounces can take a while to appear, and in this case you may see both an acceptance of the email, and later a bounce / NDR. Because the SMTP connection is no longer open, these bounces cannot be sent back to the sending server (and our platform). In this case the NDR bounces are sent to the envelope-from address (i.e. back to the customer)

1.48 I have a marketing customer who wants to use the same sending domain for SMTP transactional emails

It is important to keep separation between both use cases. The reputation of the IP address and the domain all play a role in getting email into your user's inbox rather than their spam folder. ISPs know that customers want and expect transactional emails, but it's not always easy for them to tell what's transactional and what's classified as marketing

To be on save side, the customer should use a new IP if the volume is big enough. If that is not the case, a change of the sending (sub-)domain would be good, to signal the receiving ISP/ESP that this is another traffic.

1.49 Can SMTP adapter be used for marketing emails?

SMTP relay requires multiple communications between the client and the server. This not only increases the error rate but also slows down the sending of bulk emails. REST API is often the choice of marketers dealing with bulk marketing emails. SMTP adapter can be used but it's not recommened.

1.50 Can the service recall E-Mails?

No, emails cannot be recalled

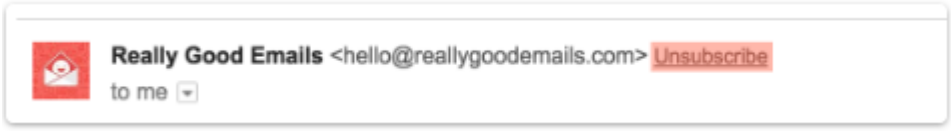
1.51 Does the service support encryption?

E-Mail 365 service supports transport level encryption using HTTPS. But application-level end to end encryption such as PGP or S/MIME is currently not supported

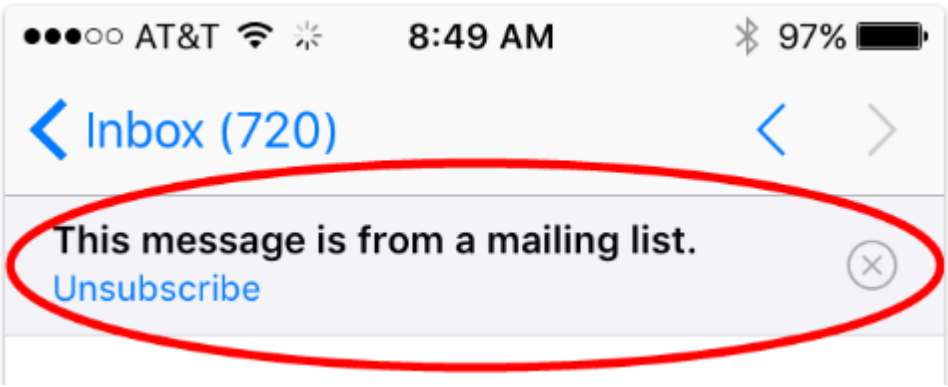
1.52 How is unsubscribe supported? Details on List unsubscribe

Customers can include unsubscribe as a direct opt-out link in the email body or as a list unsubscribe through email header (or both).
If the customer decides to use list unsubscribe through email header, they can do it two ways - As a link (utl) in the header, Or as an email address (i.e. a mailto link) in the header

Lists unsubscribe through email header is a native and easier way for users to unsubscribe, as the user doesn't need to search the email body for an unsubscribe link. How exactly list-unsubscribe displays depends on the inbox provider. Gmail, for example, displays list-unsubscribe as a text link next to the email sender information.



Others might include this as unsubscribe banner or a button e.g. iOS



1.53 How does mail-to list unsubscribe work?

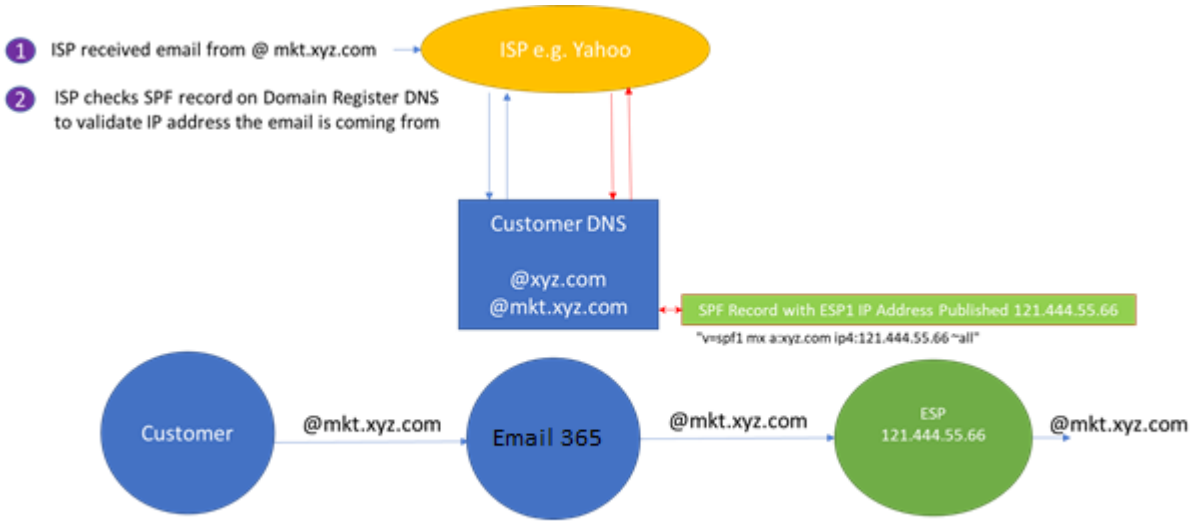
- When a recipient triggers the list-unsubscribe via the mailto link, this automatically generates an email notifying the sender (on the mail-to email address) that a recipient has unsubscribed. The unsubscribe header is set up with the email address that will receive the unsubscribe requests. (this is what the email address will do)
- It will appear on in the email header. An email client can only provide a native list-unsubscribe option if it finds list-unsubscribe instructions in the email's header.
- When a customer unsubscribes, it will automatically generate an email notifying you that an email address has unsubscribed
- Monitoring the inbox will provide the customer with information on the unsubscribes

1.54 Do we Need both SPF and DKIM? What is the SPF and DKIM flow?

Although both SPF and DKIM are used for authentication, they use different methods for email authentication.

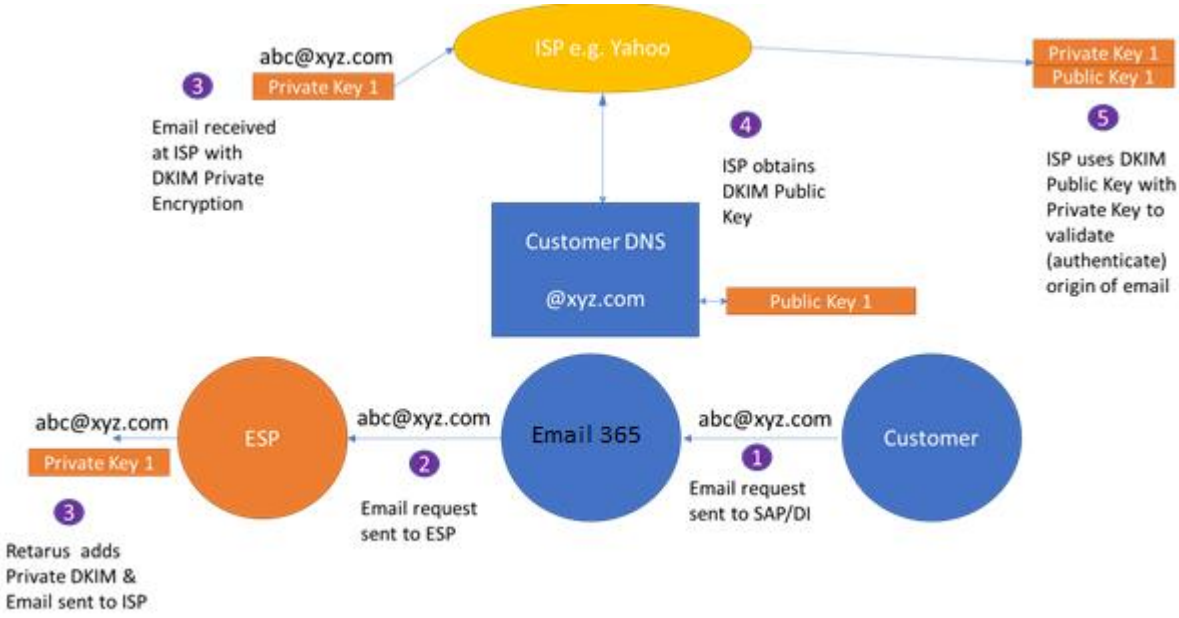
SPF defines a process to authenticate an email message that has been sent from an authorized mail server. **It compares the email sender's actual IP address to a list of IP addresses authorized to send mail from that domain. The IP list is published in the domain's DNS record.** The owner of a domain can identify which mail servers they are able to send from.

- SPF is “path-based” authentication system because it’s tied to the path the message took to get from its origin to its destination.
- SPF policies are declared in DNS TXT records.
- Based on where the message is coming from the receiving server will decide if the sending server is authorized to send the message (nothing to do with the content of the message)



DKIM uses “public key cryptography” to verify that an email message was sent from an authorized mail server. **DKIM works by adding a digital signature to the headers of an email message**.

- DKIM is referred to as “content-based” authentication because is based on whether or not the content has changed between the time it was signed and the time validation was attempted.
- The sender will generate two cryptographic keys. A private key that is used in the signing of email, and a public key that is published on the sender domain DNS for use by receiving domains in attempts to validate the signature.



Both SPF and DKIM are essential.

- Some mailbox providers only support one or the other and some support both but weight one more than the other.
- DKIM protects email from being altered in transit, SPF does not.
- Many email clients (such as Yahoo!, Gmail, Outlook, and others) will check for a valid DKIM signature on incoming email as a means of recognizing the originator.

A sender has to setup both to get the best out of their email campaigns

1.55 Is our Email solution hosted on AWS Cloud Data Centre?

Email 365 is hosted in the datacentre which is in AWS Dublin and both the Email Server instance 1 the datacentres (US in Secaucus and EU in Frankfurt) are on-prem datacentres and not hosted in AWS.

1.56 Do we support DMARC?

Email spoofing can be stopped if the ESP (email service provider) from which the email message originates from, has previously published the records. If the customer adds the ESP specified SPF and the DKIM public key in the DNS of their domain then publishing the DMARC is an added layer of security to stop spoofing of the e-mail

- SPF (Sender Policy Framework) record gives email receivers the ability to check if an email message comes from an IP address authorized by the email domain owner.
- DKIM (Domain Keys Identified Mail) record gives email receivers the ability to check if an email message was altered during its commute to the recipient.
- DMARC (Domain-based Message Authentication, Reporting and Conformance) record specifies what email receivers should do to messages that fail the previous two authentication mechanisms: Do nothing or Reject or Quarantine the message.

1.57 What is this new URL change in Email 365 ?

The current URL which was used to send requests to Email 365 to send/relay emails and receive bounce notifications will change to a new URL. Sinch has now released the functionality to allow customers to update their email services with the new revised connectivity. This change allows for the current E-Mail 365 service which had been processed on the SAP endpoints to be moved to the Sinch endpoints.
These changes have been implemented to allow for the changes in the configurations on the connections between SAP Marketing and Email 365 and be compliant with the Sinch's sets of domains and offerings. Operationally it also allows for improved and regulated scalability, robustness to the product.

E.g.,

Existing URL : https://email-eu1.sapdigitalinterconnect.com/in365-api/caas_email12345/notifications

New URL: https://eu.email.sdi.sinch.com/v1/caas_email12345/notifications

For more details please check this community link : https://community.sinch.com/t5/E-mail-365/Sinch-E-mail-365-API-Specification/td-p/2490

1.58 Who do we contact for more information?

Email 365 Support: essupport.digitalinterconnect@sinch.com
Kumar Gaurav – Sr Product Manager, kumargaurav@sinch.com
Brian Pearce – Business Senior Manager - Consulting, brian.pearce@sinch.com

Abhishek Bhandari – VP Products, abhishekb@sinch.com