Azure Meetup
TORINO

PA EXPERTISE
RETELIT GROUP

#GlobalAzureTorino

INTR3

TD SYNNEX

TORINO

Azure Meetup
TORINO

#GlobalAzureTorino

Inviare posta elettronica sicura e garantita da Azure e servizi integrati

Raffaele Colavecchi – Microsoft MVP (M365: Exchange)
Davide Rasoli – VoIP and Azure Specialist
@ Com.Tel S.p.A.

#GLOBALAZURE 2024

INTR3 TD SYNNEX PA EXPERTISE RETELIT GROUP

Agenda

- Il sottovalutato mondo della posta elettronica
  - I protocolli SPF, DKIM e DMARC
  - La Direzione di Microsoft
- Le esigenze applicative
  - ACS, SendGrid, M365 (HVE, mailbox), LogicApps
- Caso d’uso
- Q&A

Azure Meetup
TORINO

#GlobalAzureTorino

Il sottovalutato mondo della posta elettronica

#GLOBALAZURE 2024

#GlobalAzure

La storia

1981

Simple Mail Transfer Protocol (SMTP), **si comincia a spedire messaggi di posta elettronica**

1994

Tutto il mondo usa la posta elettronica, **primi abusi verificati, nasce il phishing**

2004

Sender Policy Framework (SPF), **protezione orientata ai provider di posta. GARANTISCE SOLO IL SERVER DI SPEDIZIONE**

2011

DomainKeys Identified Mail (DKIM), **autenticazione delle email in transito. GARANTISCE SOLO L'IMMODIFICABILITA' DELLA SPEDIZIONE**

2014

Domain-based Message Authentication, Reporting, and Conformance (DMARC), **protezione completa del proprio dominio GARANTISCE CHE LA MAIL PROVIENE DA FONTI ATTENDIBILI E CERTIFICATE**

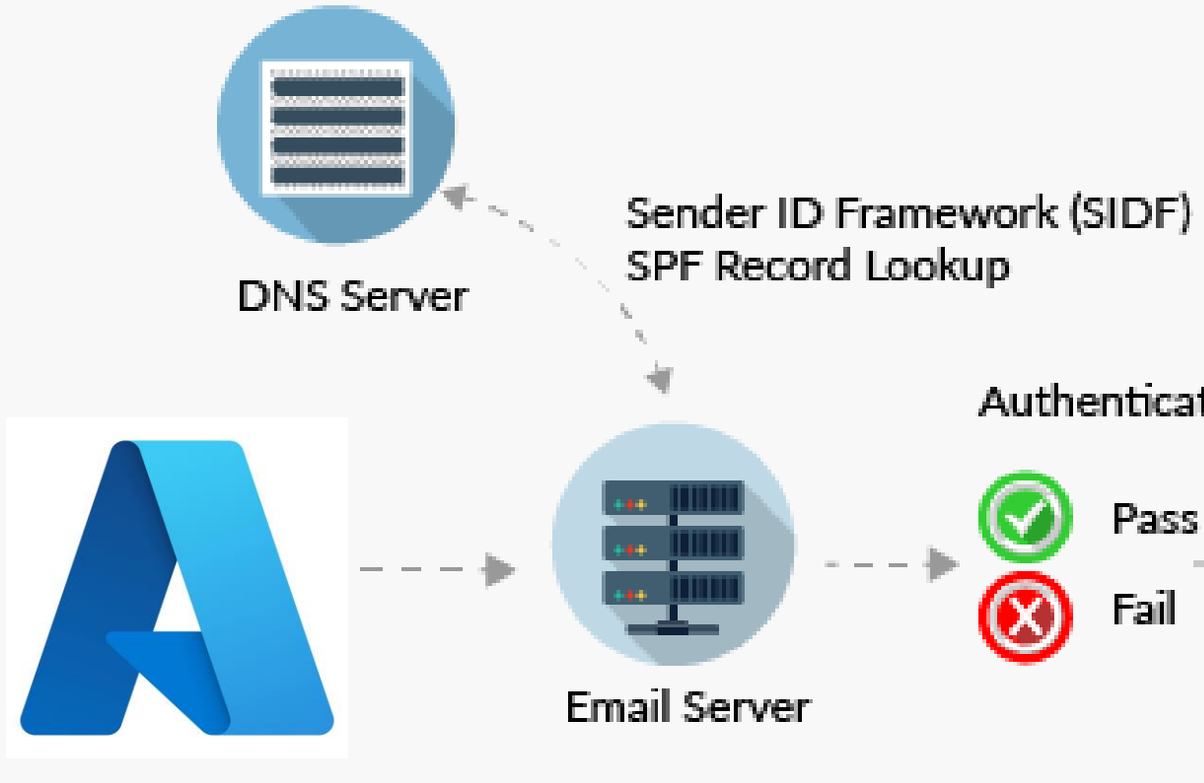
OGGI

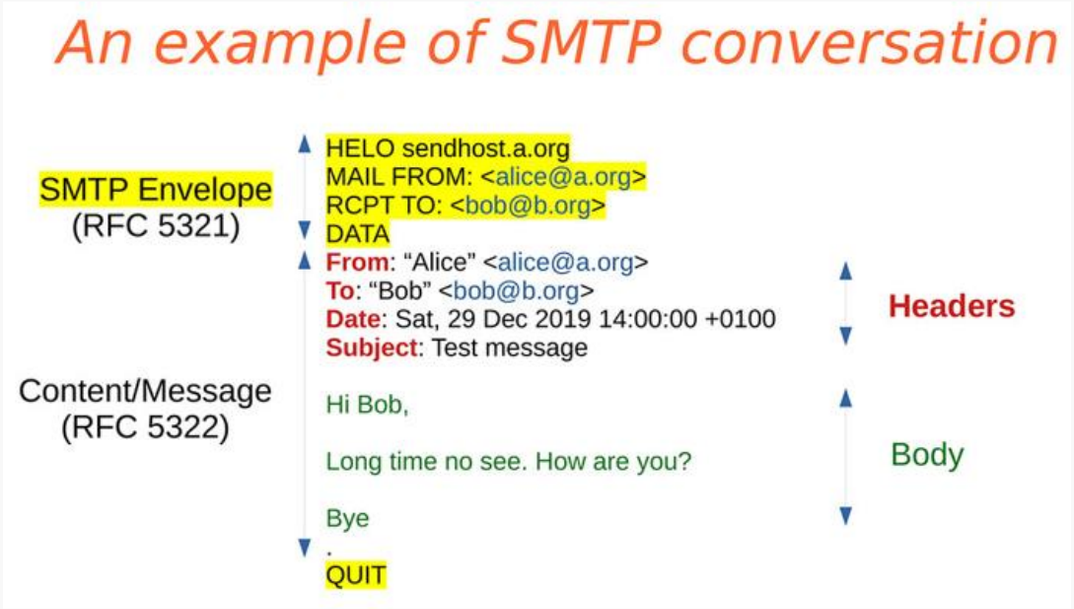
BIMI
Brand Indicators for Message Identification, **la ciliegina sulla torta.**
IL LOGO AZIENDALE

Il protocollo SPF

spf:comtelitalia.it

```
v=spf1 include:spf.protection.outlook.com ip4:85.40.208.178 -all
```





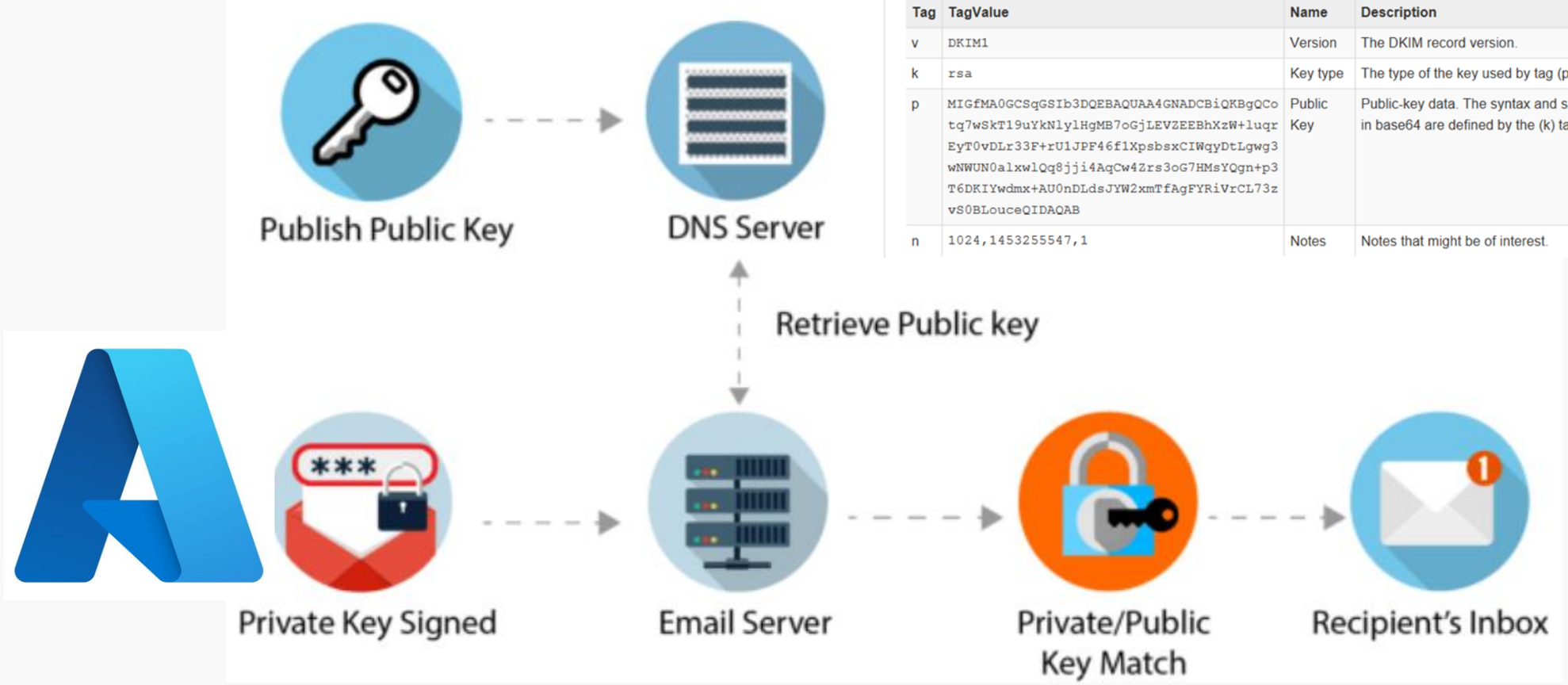
Il protocollo DKIM

dkim:exchangelabs.nl:selector1

dkim

```
v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCotq7wSkT19uYkNlylHgMB7oGjLEVZEEBhXzW+luqrEyT0vDLr33F+rU1JPF46f1X
psbsxCIWqyDtLgwg3wNWUN0alxwlQq8jji4AqCw4Zrs3oG7HMsYQgn+p3T6DKIYwdmx+AU0nDLdsJYW2xmTfAgFYRiVrCL73zvS0BLouceQIDAQAB; n=102
4,1453255547,1
```

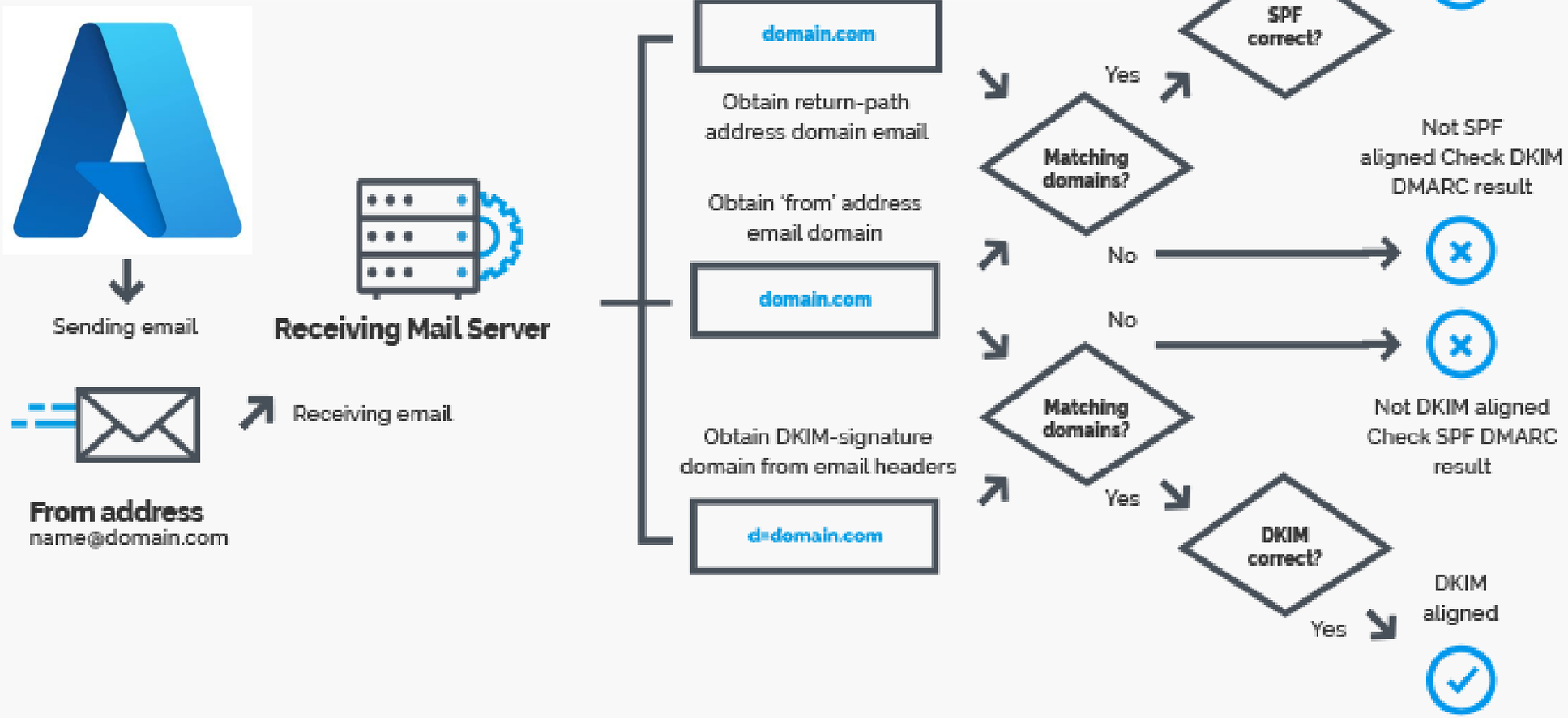
Tag	TagValue	Name	Description
v	DKIM1	Version	The DKIM record version.
k	rsa	Key type	The type of the key used by tag (p).
p	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCotq7wSkT19uYkNlylHgMB7oGjLEVZEEBhXzW+luqrEyT0vDLr33F+rU1JPF46f1XpsbsxCIWqyDtLgwg3wNWUN0alxwlQq8jji4AqCw4Zrs3oG7HMsYQgn+p3T6DKIYwdmx+AU0nDLdsJYW2xmTfAgFYRiVrCL73zvS0BLouceQIDAQAB	Public Key	Public-key data. The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.
n	1024,1453255547,1	Notes	Notes that might be of interest.



Il protocollo DMARC

dmarc:comtelitalia.it

```
v=DMARC1; p=reject; rua=mailto:xjhqpdk0@ag.eu.dmarcadvisor.com; ruf=mailto:xjhqpdk0@fr.eu.dmarcadvisor.com
```



La Direzione di Microsoft (e non solo…)

- Ridurre il numero di email
- Aumentare la qualità delle email
  - Google e Yahoo: limite dei 5000 invii giornalieri senza DMARC
  - Exchange Online: nuovi limiti per spedizioni esterne (2000 dei 10000, per utente in 24h) da Gennaio 2025
  - Exchange Online: blocco dell'autenticazione Basic over SSL per invii SMTP (porta 587) da Settembre 2025
- Nuovi protocolli all'orizzonte:
  - MTA-STS
  - SMTP DANE con DNSSEC

Le esigenze applicative

Come scegliere il servizio giusto?

Valutando prima le esigenze

Contenuto delle email

Destinatari (quantità e dove si trovano)

Protocollo di spedizione

Informazioni da raccogliere

Ricezione e gestione delle risposte

La soluzione di Microsoft 365

Microsoft High Volume Email (HVE) - Ancora in preview

Limiti di spedizione: 100’000 destinatari interni e 2’000 esterni.
Numero di caselle HVE: 20

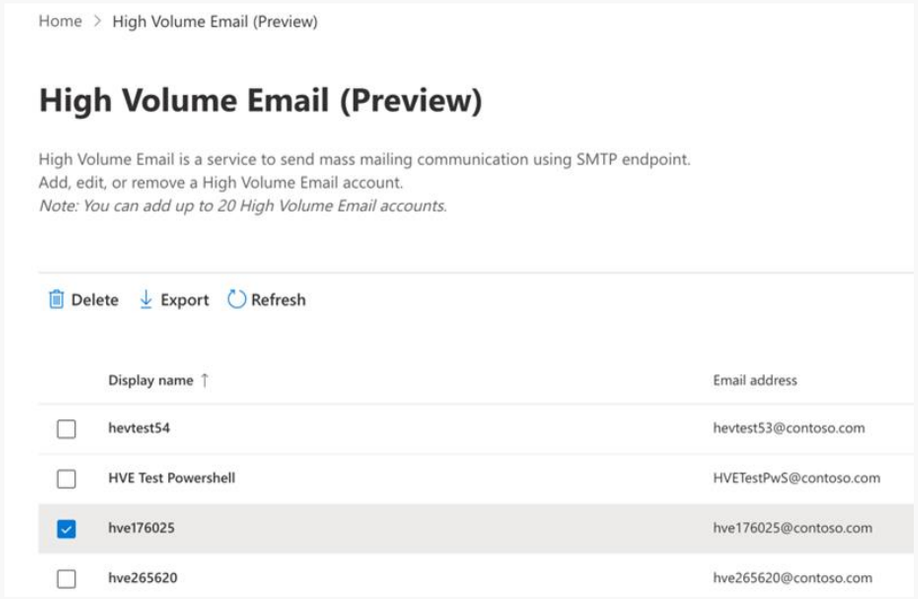
Preview (ora)	General Availability (fra 3-6 mesi)
SMTP con Basic Auth over TLS	SMTP con Basic Auth over TLS SMTP con OAUTH over TLS

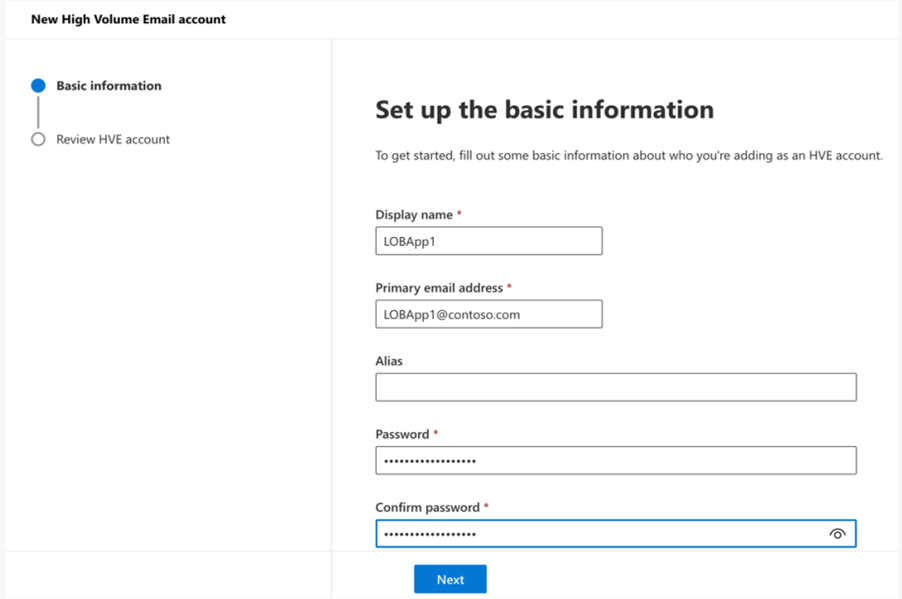
Autenticazione dei messaggi in uscita gestita da Exchange Online

Nessuna configurazione aggiuntiva di SPF e DKIM

Come si configura?

Sarà possibile configurare le caselle direttamente nell'Exchange Online admin center



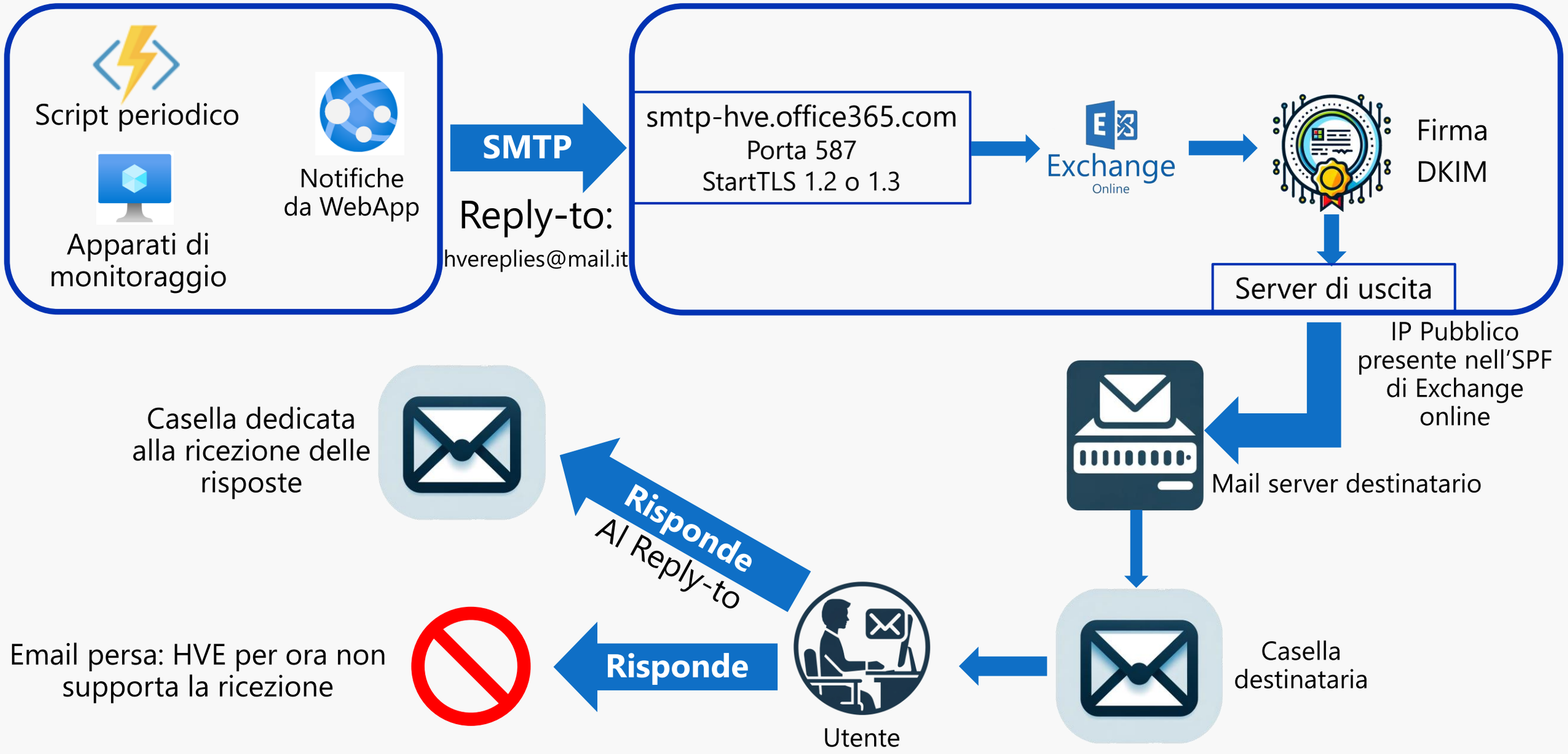


Oppure con PowerShell (modulo ExchangePowerShell)

```
PS C:\Users\Davide Rasoli> New-MailUser -LOBAppAccount -Name "Test Global Azure" -PrimarySmtpAddress "testglobalazure@comtelitalia.it"
cmdlet New-MailUser at command pipeline position 1 Supply values for the following parameters:
Password: ***************
```

```
Get-MailUser -LOBAppAccount
Set-MailUser -LOBAppAccount -Identity "testglobalazure@comtelitalia.it" -DisplayName "Test Global Azure 2"
Remove-MailUser -Identity testglobalazure@comtelitalia.it
```

Come si usa per spedire posta?



La soluzione di Azure

Email Communication Service

Limitazioni applicate
30 email inviate al minuto
100 email inviate all'ora
50 destinatari per mail
Dimensione massima di 10 MB

Per Subscription e non per singola risorsa.

Autenticazione: stessi server, ma chiavi diverse.

Aggiunta di nuovi selettori DKIM

Attenzione:

Per funzionare è richiesta anche una risorsa ACS

Funzionalità aggiuntive:

- Suppression List
- SDK per la spedizione
- Invio asincrono

Come si attiva?

Creazione della risorsa Email Communication Service in Azure

Email Communication Services

Microsoft

Azure Service

Create an Email Communication Services resource for adding email capabilities into your applications

Instance details

Name * Test-GA-Davide

Region Global

This resource is a global resource that works across Azure regions.

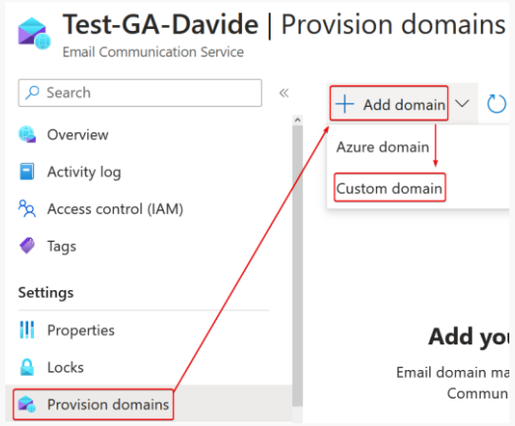
Data location Europe

Configurazione dei domini

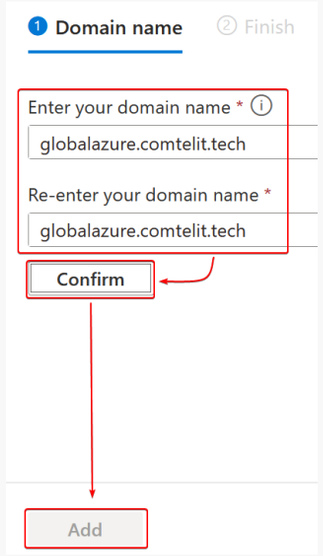
Dominio fornito da Azure

Da usare solo per test: Max 10 mail / ora

Dominio personalizzato

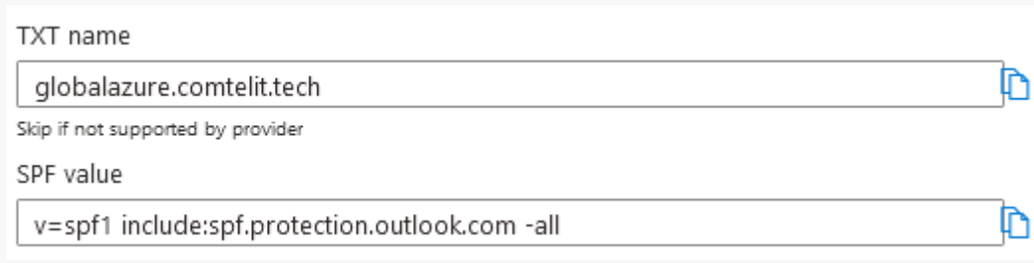


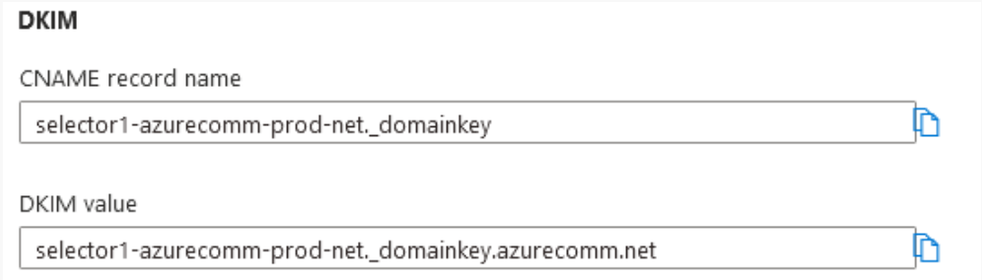
Configurazione del dominio



Verifica della proprietà

Configurazione dell'SPF



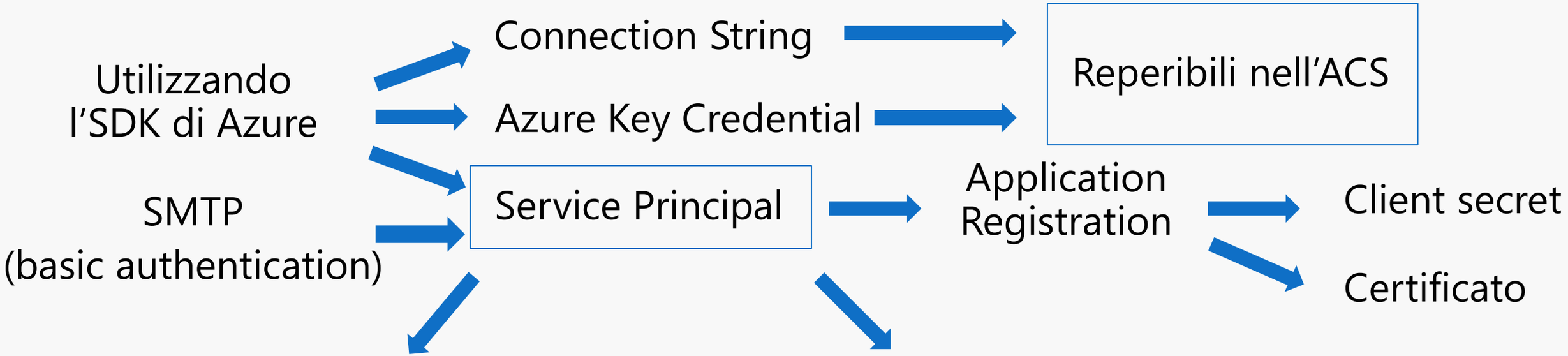


Configurazione del DKIM (attenzione ai sottodomini)

E il DMARC?

Domain name	Domain type	Domain status	SPF status	DKIM status	DKIM2 status
globalazure.comtelit.tech	Custom domain	Verified	Verified	Verified	Verified

Quali sono le modalità di spedizione?



Per spedire con SMTP, devo autorizzare sull'ACS interessato i seguenti permessi:

Permission
Microsoft.Communication/CommunicationServices/Read
Microsoft.Communication/EmailServices/write

Per spedire dall'SDK, devo autorizzare sull'ACS interessato i seguenti permessi:

Permission
Microsoft.Communication/CommunicationServices/Read
Microsoft.Communication/CommunicationServices/Write
Microsoft.Communication/EmailServices/write
Microsoft.Communication/EmailServices/read

La soluzione di terze parti, ma integrata

SendGrid

Progettato per l'invio e il tracciamento delle email commerciali.

Consigliabile se si spedisce una grande quantità di email.

Disponibili diversi piani in base a funzionalità e volume (sottoscrivibili Free, Essential e Pro)

Evitare di autenticare il singolo indirizzo mittente

Autenticare l'intero dominio, personalizzare il return-path

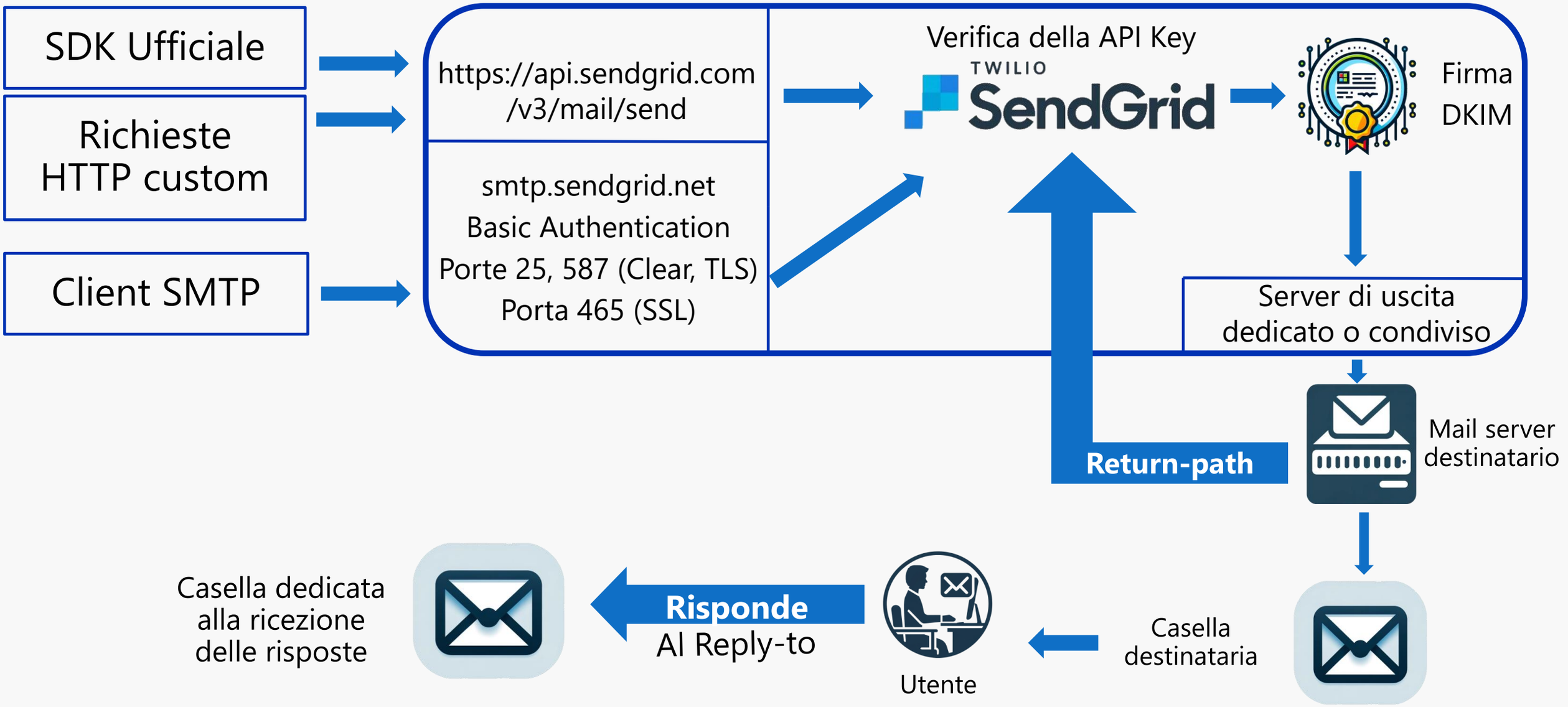
Autenticazione: server e chiavi di SendGrid

Configurazione completa

Attenzione all'IP mittente

Se possibile, utilizzare un piano con IP dedicato

Quali sono le modalità di spedizione?



Il caso d'uso

Spedizione di promemoria da una Shared Mailbox con una Logic App

LA-Promemoria

Utilizzando una managed identity

Microsoft Graph API

Lista SharePoint Online

Exchange Online

Note sul flusso autorizzativo:

- API Graph: Mail.Send

Problema di sicurezza

Soluzione: Application Access Policies di Exchange Online

Riferimenti:

Raffaele Colavecchi
Microsoft MVP (M365: Exchange)
Profilo LinkedIn
raffaele.colavecchi@comtelitalia.it

Davide Rasoli
VoIP and Azure Specialist
Profilo LinkedIn
davide.rasoli@comtelitalia.it

Azure Meetup
TORINO

#GlobalAzureTorino

TORINO

TD SYNNEX

INTR3

PA EXPERTISE
RETELIT GROUP