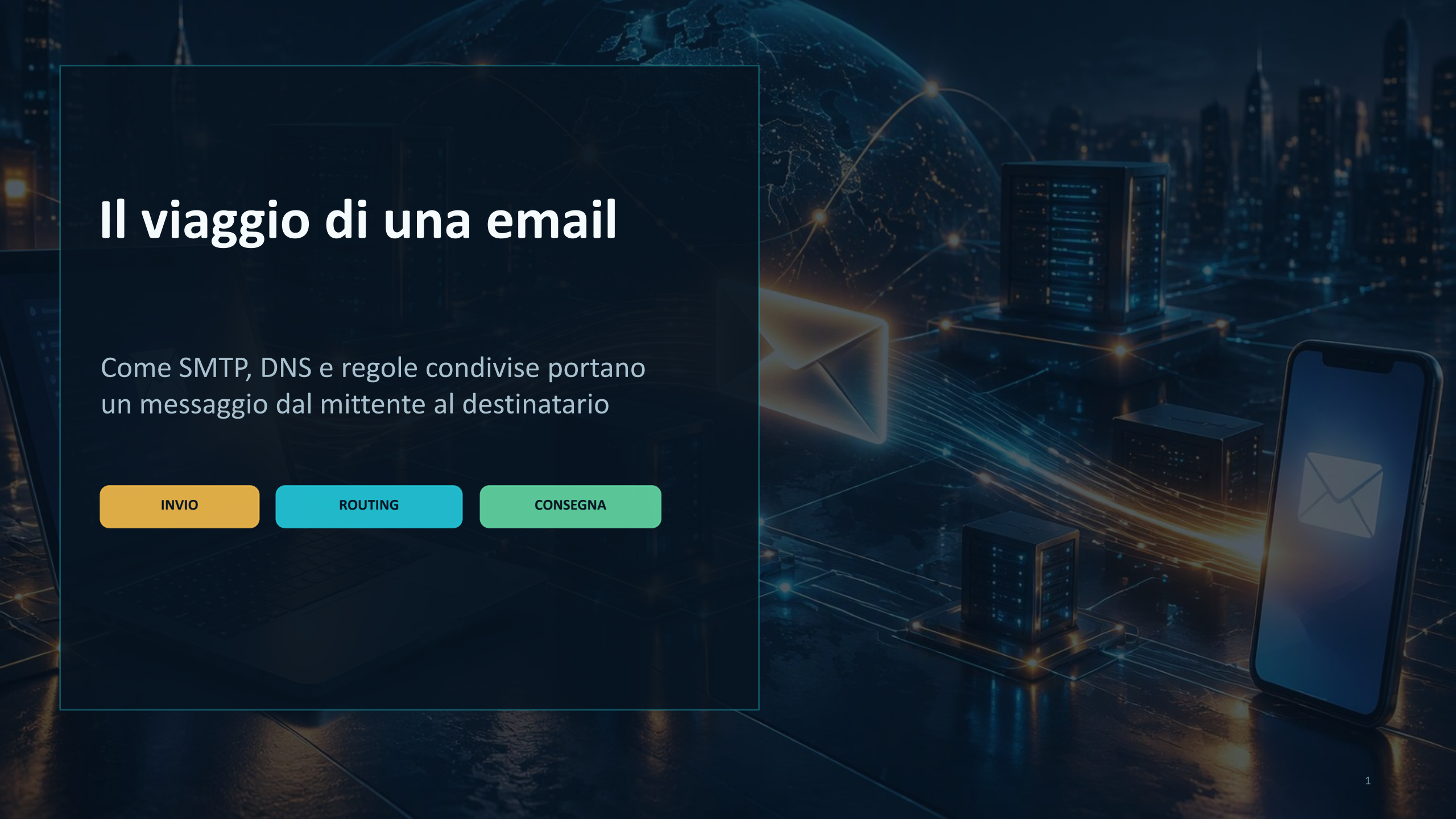
Il viaggio di una email

Come SMTP, DNS e regole condivise portano un messaggio dal mittente al destinatario

INVIO | ROUTING | CONSEGNA



EMAIL SU INTERNET: UN PROTOCOLLO, DECENNI DI EVOLUZIONE

Da una delle prime applicazioni di rete a un'infrastruttura critica ancora in evoluzione

1971
Prima email in ARPANET
Ray Tomlinson invia la prima email

1982
SMTP e formato messaggio
RFC 821 (SMTP)
RFC 822 (formato messaggio)

1983
Adozione di TCP/IP su ARPANET
DNS prende forma (RFC 882/883)

1990s
MIME, POP3, IMAP e prime estensioni
RFC 2045–2049 (MIME)
RFC 1939 (POP3)
RFC 2060 (IMAP)

2000s
Standard consolidati
RFC 5321 (SMTP)
RFC 5322 (messaggio)

2010s
Autenticazione e TLS più robusti
SPF, DKIM, DMARC
STARTTLS, MTA-STS, DANE

2020s – 2026
Sicurezza, policy e report aggiornati
RFC 8461, RFC 9989

EMAIL:
utenti ↔ host ↔ host

TRASPORTO SMTP
Consegna tra host
- RFC 821 (1982)
- RFC 2821 (2001)
- **RFC 5321** (2008) SMTP

FORMATO MESSAGGIO
Intestazioni e sintassi
- RFC 822 (1982)
- RFC 2822 (2001)
- **RFC 5322** (2008) Header

CONTENUTI E CASELLE
Allegati, MIME e accesso alla posta
- MIME RFC 2045–2049 (1996)
- POP3 RFC 1939 (1996)
- IMAP4rev2 RFC 9051 (2021)

INVIO E ACCESSO
Porte standard e submission
- 587 Submission + STARTTLS
- 465 Submission TLS implicito
- 110 POP3 (non cifrato)
- 995 POP3 TLS implicito
- 143 IMAP (non cifrato)
- 993 IMAP TLS implicito

AUTENTICAZIONE DOMINIO
Antispoofing e antispam
- SPF RFC 7208 (2014)
- DKIM RFC 6376 (2011)
- DMARC RFC 9989 (2026)

SICUREZZA TRASPORTO
Cifratura e protezione del collegamento
- STARTTLS RFC 3207 (2002)
- MTA-STS RFC 8461 (2018)
- DANE RFC 7672 (2015)
- TLS 1.3 RFC 8446 (2018)

Le RFC non sono scolpite nella pietra: evolvono per interoperabilità, sicurezza e nuove minacce.

STARTTLS è un'estensione del protocollo, non una porta. Le porte indicano servizi convenzionali.

Che cosa succede dopo l'invia"?

In pochi secondi entrano in gioco più sistemi, ognuno con un compito preciso.

1. Il client prepara

Corpo, allegati, destinatari e intestazioni

2. Il server prende in carico

Accetta il messaggio e decide dove inoltrarlo

3. Il DNS indica la strada

Il record MX identifica il sistema ricevente

4. Il destinatario controlla

Identità, reputazione, malware e policy

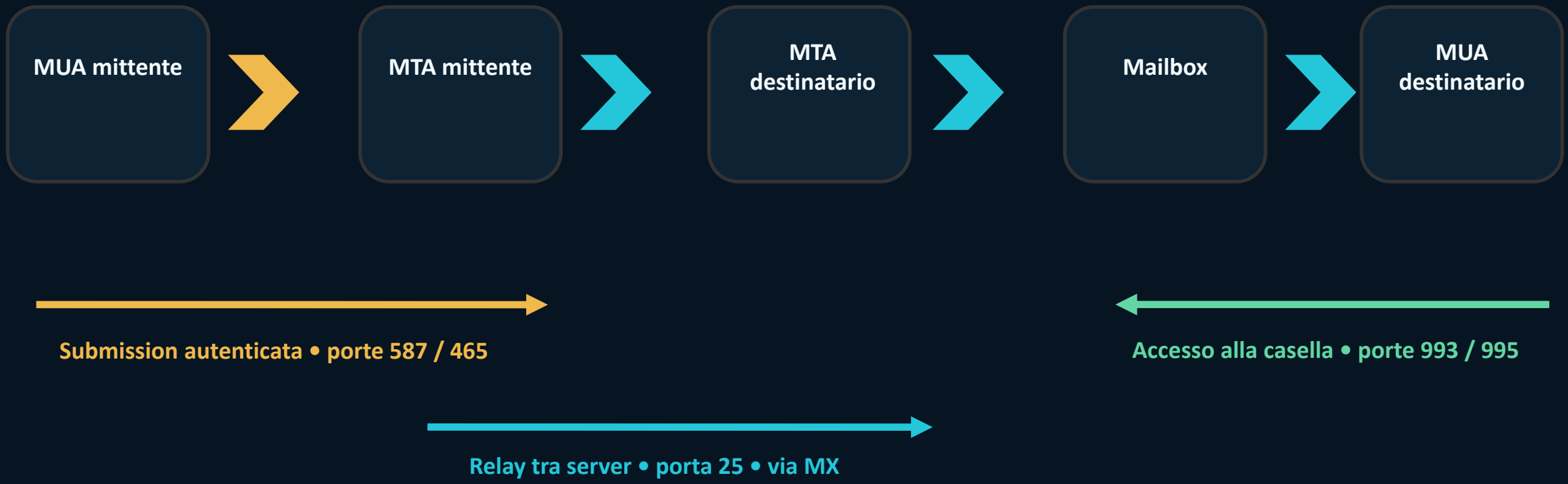
5. La mailbox conserva

La posta viene depositata e resa disponibile via webmail o app client

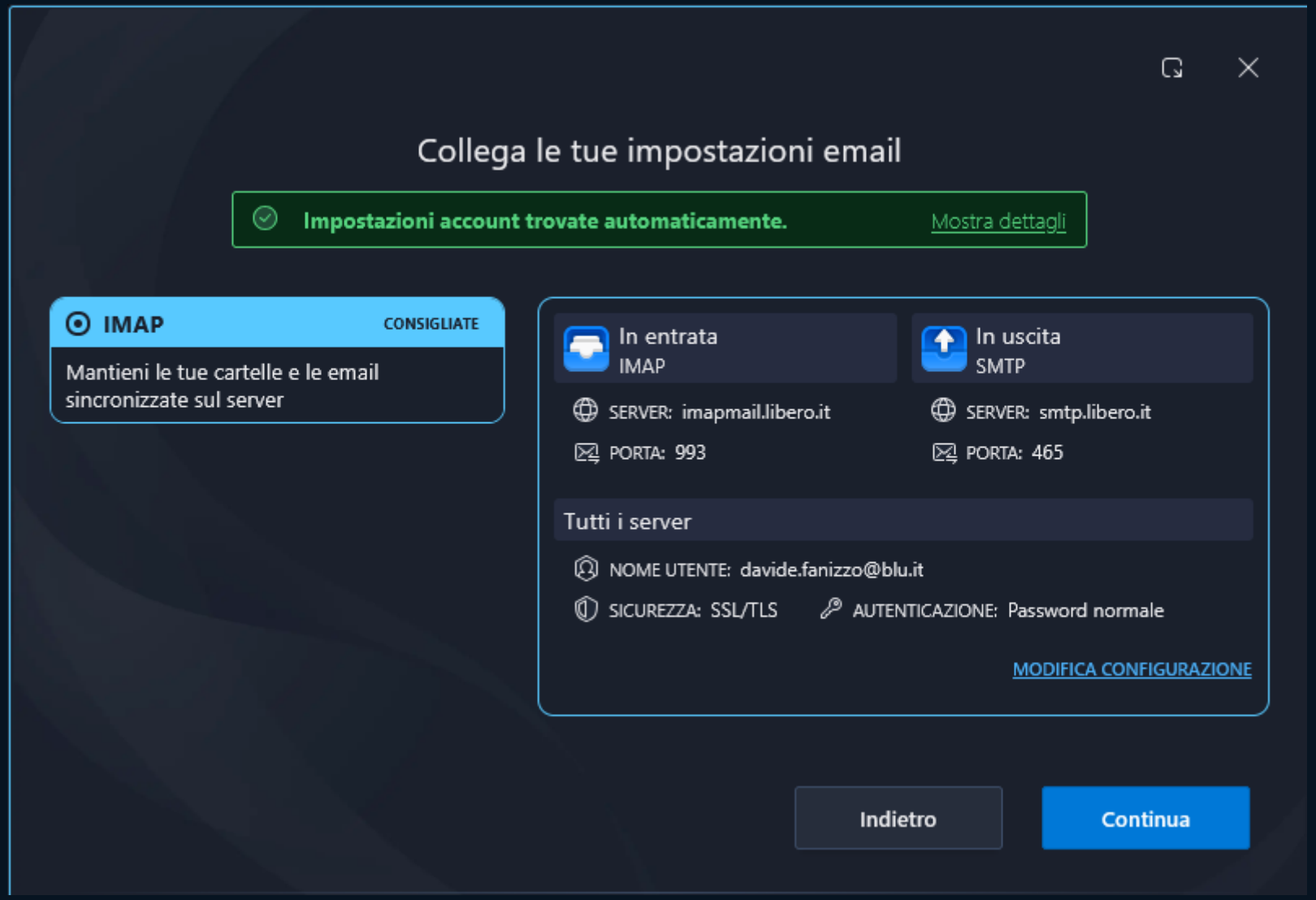


Due conversazioni diverse

Il client non parla con il destinatario finale: consegna prima al proprio server.



Impostazione client di posta (MUA)



SMTP è una conversazione

Comandi semplici, risposte numeriche e una sequenza molto rigorosa.

220	Server pronto
EHLO	Mi presento e chiedo le funzionalità
250	Ecco cosa supporto
STARTTLS	Passiamo a un canale cifrato
MAIL FROM	Mittente della busta SMTP
RCPT TO	Destinatario della busta SMTP
DATA / BDAT	Contenuto del messaggio
250	Messaggio accettato in coda



2xx = successo • 4xx = problema temporaneo • 5xx = rifiuto definitivo

TLS protegge il viaggio

Implicito oppure con commando STARTTLS cifra la sessione tra due server



Cosa protegge

Contenuto e credenziali mentre attraversano quella tratta di rete

Cosa verifica

Protocollo, cipher e certificato secondo la policy del mittente

Cosa non garantisce

Che il campo From sia autentico o che il messaggio sia innocuo

Ogni tratta può avere una protezione diversa

Gli header: la “scatola nera” di una e-mail

Metadati scritti dal client e dai server: identità dichiarata, percorso, autenticazione e formato del contenuto.

ESEMPIO SEMPLIFICATO

From:	Alice <alice@example.org>
To:	Bob <bob@example.net>
Subject:	Serata Hacklab
Date:	Wed, 28 Oct 2026 20:30:00 +0100
Message-ID:	<abc123@example.org>
Return-Path:	<bounce@example.org>
Received:	from mail.example.org by mx.example.net
	with ESMTPS id 42; Wed, 28 Oct 2026 20:30:03 +0100
Authentication-Results:	mx.example.net;
	spf=pass; dkim=pass; dmarc=pass
DKIM-Signature:	v=1; d=example.org; s=mail; ...
Content-Type:	text/plain; charset=UTF-8
riga vuota	**Da qui inizia il corpo del messaggio**

1 Ciò che vede l’utente

From, To, Subject e Date sono header RFC 5322. Il campo From è distinto dal MAIL FROM della busta SMTP.

2 Il percorso

Ogni sistema ricevente aggiunge una riga Received in cima. Per seguire il viaggio si leggono le righe Received dal basso verso l’alto.

3 I controlli

Authentication-Results registra gli esiti osservati dal receiver: SPF, DKIM, DMARC e altri meccanismi.

4 Integrità e formato

DKIM-Signature firma header e corpo selezionati. Content-Type e MIME descrivono testo, HTML e allegati.

Regola pratica un header racconta ciò che ogni hop ha dichiarato o osservato; va interpretato nel contesto della catena.

Il DNS è il navigatore della posta

Prima della connessione SMTP, il mittente deve trovare il server che riceve per quel dominio.



MX

Indica quali host ricevono la posta del dominio destinatario

A / AAAA

Traduce il nome dell'host nell'indirizzo IP

TXT

Contiene policy e chiavi usate da SPF, DKIM e DMARC del dominio mittente

Priorità più bassa = server preferito

Il destinatario prende una decisione

L’autenticazione è solo una parte: contano anche reputazione, contenuto e policy locali.



Lo stesso messaggio può essere accettato da un’organizzazione e messo in quarantena da un’altra.

DNSBL / RBL: reputazione dell’IP mittente

Una query DNS velocissima aiuta il server ricevente a valutare la connessione SMTP.

1. Osserva l’IP

Il controllo riguarda l’IP che apre la sessione SMTP, non l’indirizzo visibile nel campo From.

2. Interroga la DNSBL

Il server costruisce un nome DNS usando gli ottetti dell’IPv4 in ordine inverso.

3. Legge la risposta

NXDOMAIN indica normalmente “non presente”. Un record A 127.x.x.x può indicare una lista o un errore.

4. Applica una policy

La presenza in lista può aumentare lo spam score, causare quarantena o rifiuto, secondo la configurazione locale.

Importante: DNSBL ≠ prova definitiva di spam

È un segnale reputazionale da combinare con identità, contenuto e policy.



ZEN riunisce SBL, CSS, XBL e PBL in un’unica zona DNSBL.

Come interrogare Spamhaus ZEN

Dall’IP trovato negli header alla query DNS e all’interpretazione del risultato.

IP della connessione SMTP

213.209.10.16

Inverti gli ottetti

16.10.209.213

Aggiungi la zona DNSBL

16.10.209.213.zen.spamhaus.org

```
nslookup -type=A 16.10.209.213.zen.spamhaus.org
```

NXDOMAIN

In genere: IP non presente nella zona interrogata.

127.x.x.x

Risposta da interpretare usando il codice restituito.

- L’indirizzo mail non entra nella query: serve l’IP del server che ha consegnato la mail.
- Un risultato “listed” non dimostra da solo che quella specifica mail sia spam.
- 127.255.255.254 e 127.255.255.255 sono errori di interrogazione, non risultati reputazionali.

Tre controlli contro lo spoofing

SPF, DKIM e DMARC lavorano insieme, ma controllano aspetti differenti.

SPF

L'IP che consegna è autorizzato dal dominio della busta?

DKIM

La firma crittografica del dominio è valida e il contenuto è integro?

DMARC

Il dominio visibile nel From è allineato con SPF o DKIM? Quale policy applicare?

PASS non significa "messaggio sicuro". Significa che identità e policy hanno superato quel controllo.



Report DMARC: vedere chi usa il tuo dominio

I receiver trasformano i risultati SPF, DKIM e DMARC in telemetria inviata agli indirizzi dichiarati nel record DNS.



RUA • aggregati

File XML periodici: volumi per IP, disposition, risultati SPF/DKIM e allineamento.

RUF • failure

Dettagli su singoli fallimenti. Disponibilità limitata, con implicazioni di privacy.

Record DNS di esempio

`v=DMARC1; p=none; rua=mailto:dmarc@example.org`

INVENTARIO

Quali IP e servizi inviano per noi?

CORREZIONE

SPF, chiavi DKIM, allineamento e flussi indiretti

ENFORCEMENT

Passaggio prudente da p=none a quarantine/reject

Un report non blocca nulla: fornisce visibilità per correggere prima di applicare una policy più severa.

NDR: quando la consegna non riesce

Il rapporto di mancata consegna è un nuovo messaggio generato da un MTA, non la risposta del destinatario.

1. **Tentativo** — Il mittente consegna al proprio MTA
2. **Errore** — Il server remoto rifiuta oppure non risponde
3. **Retry** — Un errore 4xx resta in coda e viene riprovato
4. **NDR** — Dopo un 5xx o il timeout viene notificato il mittente



4xx = temporaneo

Coda, retry e possibile NDR solo al timeout.

5xx = definitivo

Rifiuto permanente e NDR normalmente immediato.

Enhanced status code

Esempio: 5.1.1 destinatario inesistente.

Quando qualcosa non funziona

Dov’è il problema?

1. **DNS** — MX corretto? IP raggiungibile?
2. **Connessione** — TCP 25 aperta? Quale server risponde?
3. **TLS** — STARTTLS, protocollo, cipher, certificato
4. **SMTP** — Ultimo comando e codice 4xx/5xx
5. **Messaggio** — Message-ID, header Received, trace e code



Gli header: la “scatola nera” di una e-mail

Metadati scritti dal client e dai server: identità dichiarata, percorso, autenticazione e formato del contenuto.

ESEMPIO SEMPLIFICATO

From:	Alice <alice@example.org>
To:	Bob <bob@example.net>
Subject:	Serata Hacklab
Date:	Wed, 28 Oct 2026 20:30:00 +0100
Message-ID:	<abc123@example.org>
Return-Path:	<bounce@example.org>
Received:	from mail.example.org by mx.example.net
	with ESMTPS id 42; Wed, 28 Oct 2026 20:30:03 +0100
Authentication-Results:	mx.example.net;
	spf=pass; dkim=pass; dmarc=pass
DKIM-Signature:	v=1; d=example.org; s=mail; ...
Content-Type:	text/plain; charset=UTF-8
riga vuota	**Da qui inizia il corpo del messaggio**

1 Ciò che vede l’utente

From, To, Subject e Date sono header RFC 5322. Il campo From è distinto dal MAIL FROM della busta SMTP.

2 Il percorso

Ogni sistema ricevente aggiunge una riga Received in cima. Per seguire il viaggio si leggono le righe Received dal basso verso l’alto.

3 I controlli

Authentication-Results registra gli esiti osservati dal receiver: SPF, DKIM, DMARC e altri meccanismi.

4 Integrità e formato

DKIM-Signature firma header e corpo selezionati. Content-Type e MIME descrivono testo, HTML e allegati.

Regola pratica un header racconta ciò che ogni hop ha dichiarato o osservato; va interpretato nel contesto della catena.

IL VIAGGIO DI UNA EMAIL

Dal mittente al destinatario: tutti i passaggi, le verifiche e i protocolli coinvolti

1 MUA Mittente

Scrive e invia l'email

Client di posta (es. Thunderbird, Outlook, webmail)

- Composizione del messaggio
- Indirizzi, oggetto, allegati (MIME)
- Invio al server di submission

2 MTA Submission

Riceve l'email dal mittente

Server di submission del provider

- Autenticazione utente (SMTP AUTH)
- Porta 587 (STARTTLS) o 465 (TLS implicito)
- Controlli iniziali (virus, policy, dimensione)
- Aggiunge intestazioni Received

3 DNS Record MX

Trova il server del dominio del destinatario

Query DNS per MX

```
$ dig MX destinatario.it

destinatario.it. 3600 IN MX 10 mail1.destinatario.it.
destinatario.it. 3600 IN MX 20 mail2.destinatario.it.
```

- Il record MX indica quali server ricevono la posta per il dominio
- Viene risolto in un indirizzo IP

4 MTA Destinatario

Riceve la connessione SMTP e inizia le verifiche

Connessione SMTP

- Il server mittente si connette al server del destinatario (porta 25)
- EHLO, scambio di capacità
- Inizio controlli di sicurezza

5 Verifiche di autenticazione (query DNS)

SPF — Query DNS record TXT
es. destinatario.it
v=spf1 ip4:... include:... -all

DKIM — Query DNS record TXT
es. selector._domainkey.destinatario.it
v=DKIM1; k=rsa; p=...

DMARC — Query DNS record TXT
es. _dmarc.destinatario.it
v=DMARC1; p=quarantine; ...

6 Controlli antispam e reputazione

RBL / DNSBL
Query a database di reputazione IP (es. Spamhaus, Spamcop, ecc.)

Analisi contenuto
- Filtri antispam
- Analisi euristica
- Rilevamento virus
- Controllo allegati
- Policy locali

Altri controlli
- Greylisting
- Rate limiting
- Reputazione dominio
- Lista safe/blocked
- Controlli specifici del provider

7 Accettazione e consegna

- Se tutti i controlli sono superati, il messaggio viene accettato (codice 250)
- L'MTA consegna il messaggio al Mail Delivery Agent (MDA)

8 Deposito su server mail

Il messaggio viene archiviato nella casella del destinatario

- Consegna locale al server IMAP/POP3
- Organizzazione in cartelle (Inbox, Spam, ecc.)
- Indicizzazione e disponibilità per la lettura

9 MUA Destinatario

Legge l'email

- Accesso alla casella tramite IMAP o POP3
- Porte standard:
  - IMAP 143 (STARTTLS)
  - IMAP 993 (TLS implicito)
  - POP3 110 (STARTTLS)
  - POP3 995 (TLS implicito)
- Visualizzazione del messaggio e degli allegati



Principali porte e protocolli

25	SMTP	Trasporto tra server (MTA ↔ MTA)
587	Submission SMTP	Invio dal client al server (STARTTLS)
465	Submission SMTP	Invio dal client al server (TLS implicito)
110	POP3	Lettura della posta (STARTTLS)
995	POP3	Lettura della posta (TLS implicito)
143	IMAP	Lettura della posta (STARTTLS)
993	IMAP	Lettura della posta (TLS implicito)

DNS record utilizzati

MX	Indica i server che ricevono la posta per il dominio
TXT (SPF)	Elenco degli IP autorizzati a inviare
TXT (DKIM)	Chiave pubblica per verificare la firma del messaggio
TXT (DMARC)	Policy e report per l'autenticazione del dominio

Cinque idee da portarsi a casa

1	**SMTP trasporta**	Non è la mailbox e non è il client.
2	**DNS instrada**	Il record MX indica dove consegnare.
3	**TLS cifra**	Protegge la tratta, non certifica il From.
4	**SPF/DKIM/DMARC valutano**	Autorizzazione, firma, allineamento e policy.
5	**Gli header raccontano il viaggio**	Received, codici SMTP e timestamp ricostruiscono il percorso e le tempistiche

Domande?