Arquitectura y Funcionamiento de los Servidores de Correo

Deconstrucción técnica del servicio de red más utilizado del mundo.

Definición: Un servicio de red asíncrono basado en el modelo cliente/servidor que permite el intercambio de mensajes digitales a través de redes de transmisión de datos.

Orígenes: FTP

1982: SMTP (RFC 821)

Actualidad: ESMTP / RFC 2821

Los Actores del Sistema: MUA, MTA y MDA

MUA (Mail User Agent)

Cliente / Remitente

Interfaz que permite al usuario componer, enviar y leer correos.

Analogía: El escritorio o buzón personal.

Ej: Outlook, Thunderbird, Gmail Web

MTA (Mail Transfer Agent)

Servidor de Transporte

Encarga del encaminamiento y transferencia entre sistemas (SMTP).

Analogía: Oficina de correos y transporte.

Ej: Postfix, Exchange, Sendmail

MDA (Mail Delivery Agent)

Agente de Entrega

Recibe el correo del MTA y lo deposita en el buzón final.

Analogía: El cartero local.

Technical Manual meets Swiss Design

El Ciclo de Vida de un Email: 5 Pasos Críticos

1. Creación

Usuario redacta en MUA.

2. Almacén de Salida

Espera en Outbox.

3. Petición de Envío (Push)

MTA origen contacta MTA destino.

4. Validación y Recepción

Validación y entrega a MDA.

5. Recuperación (Pull)

Destinatario descarga mensaje.

PUSH (Envío)

PULL (Recogida)

Protocolo SMTP: El Motor del Transporte

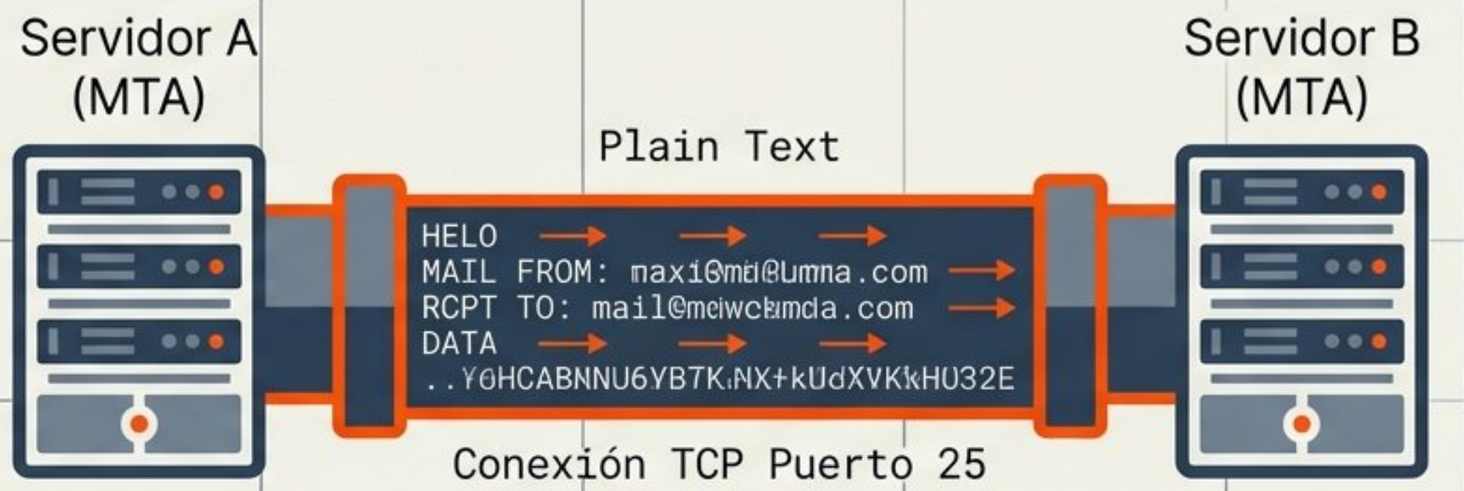
Ficha Técnica

Nombre: Simple Mail Transfer Protocol

Estándar: RFC 2821

Puerto: 25 (TCP)

Formato: Texto ASCII



- **Función:** Transmisión de correo entre servidores (MTA a MTA).
- **Método:** Protocolo “Push” (Empujar).
- **Vulnerabilidad:** Sin autenticación nativa. Origen del SPAM.

La Conversación SMTP: Comandos y Respuestas

Terminal Window

```
C: HELO mi.dominio.com
S: 250 OK Hello
C: MAIL FROM: <ana@a.org>
S: 250 OK
C: RCPT TO: <bea@b.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: [Contenido del Mensaje]
C: .
S: 250 OK
C: QUIT
```

Códigos de Estado

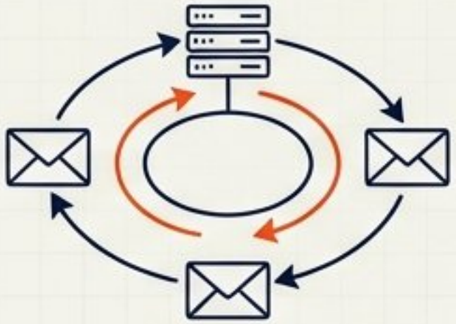
250: Éxito / Acción completada

421: Error Temporal (Servicio no disponible)

550: Error Permanente (Usuario desconocido)

Evolución y Corrección: ESMTP

El Problema: SMTP Original (RFC 821)

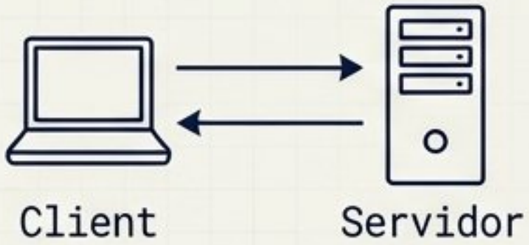


- Límite de mensaje: 64KB

- Timeouts frecuentes

- Bucles infinitos (Tormentas de correo)

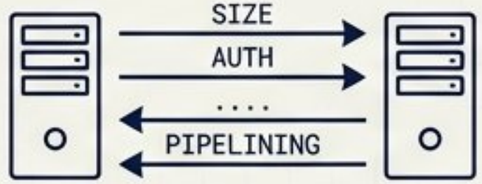
La Solución: ESMTP (RFC 1425)



- Soporte para extensiones y multimedia

- Nuevo Saludo: EHLO

- Negociación de capacidades



Compatibilidad: Si el servidor rechaza EHLO, el cliente vuelve automáticamente a HELO.

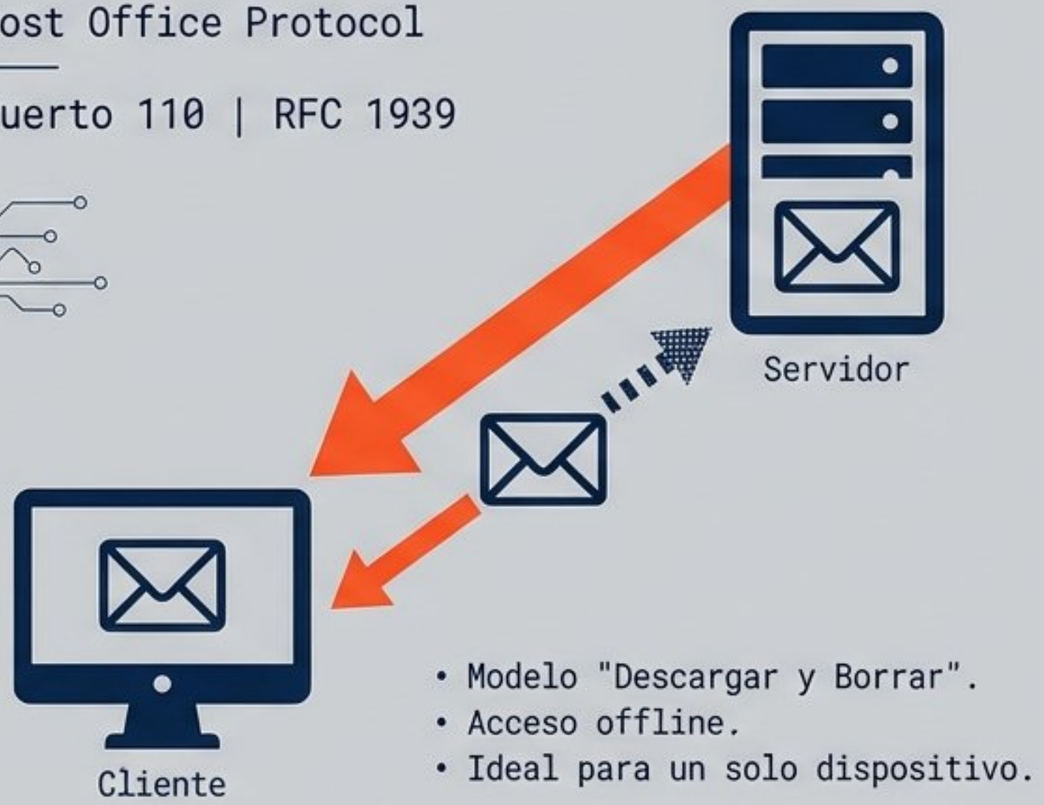
Reference RFCs: RFC 821, RFC 1425, RFC 1869, RFC 1911, RFC 1651, RFC 1830, RFC 3030, STD0010.

Protocolos de Acceso: ¿POP3 o IMAP?

POP3

Post Office Protocol

Puerto 110 | RFC 1939



- Modelo "Descargar y Borrar".
- Acceso offline.
- Ideal para un solo dispositivo.

IMAP

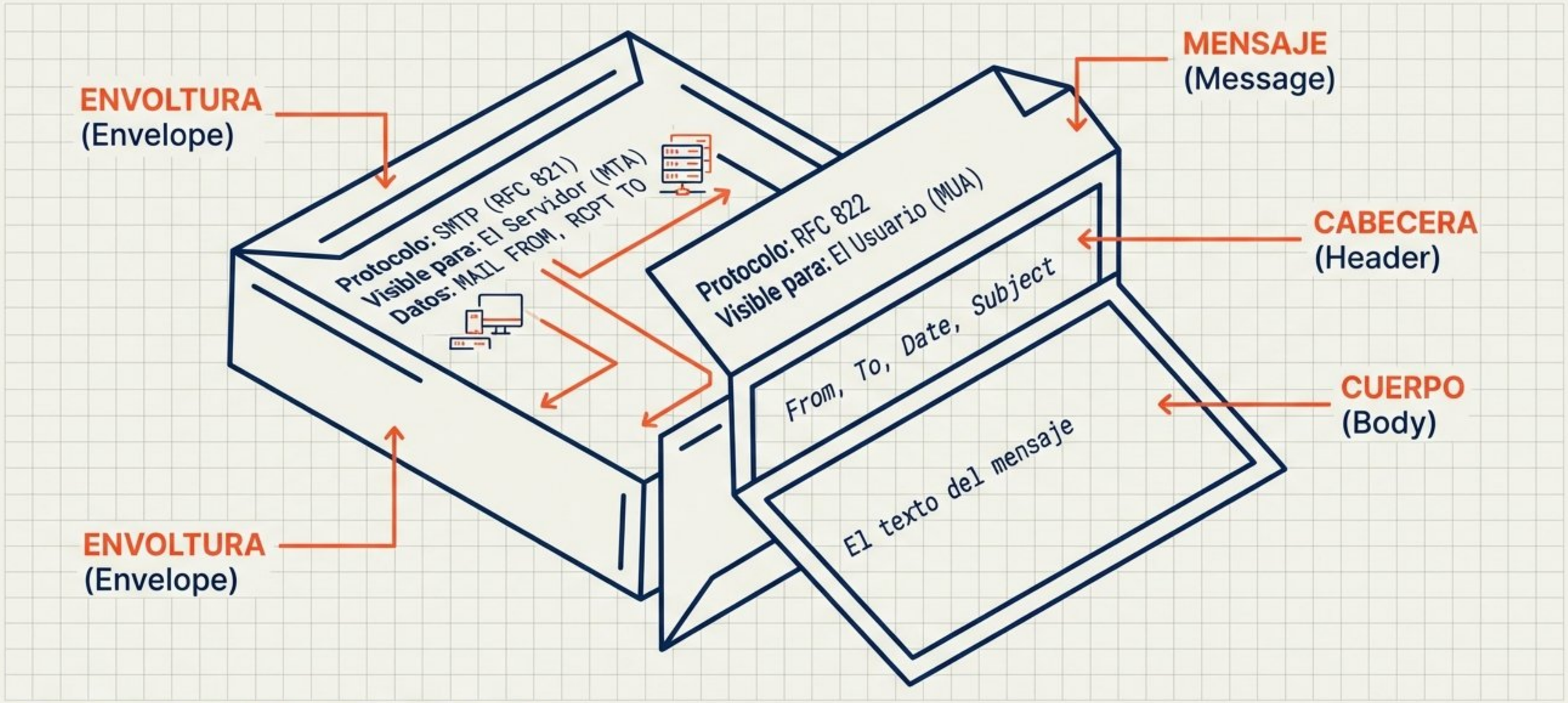
Internet Message Access Protocol

Puerto 143 | RFC 3501

- Modelo "Gestión Remota".
- El correo vive en el servidor.
- Sincronización multidispositivo.

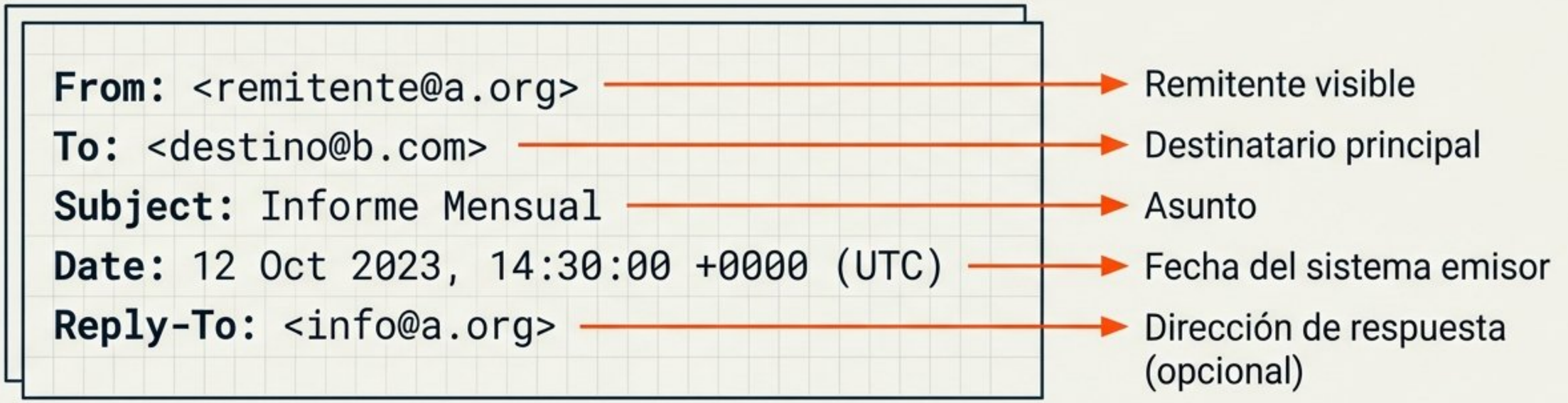
Technical Manual meets Swiss Design. Reference Schematic: <IMAGE_0>

Anatomía del Mensaje: Envoltura vs. Contenido



Technical Manual meets Swiss Design. Reference Schematic: <IMAGE_0>

Desglosando las Cabeceras (RFC 822)



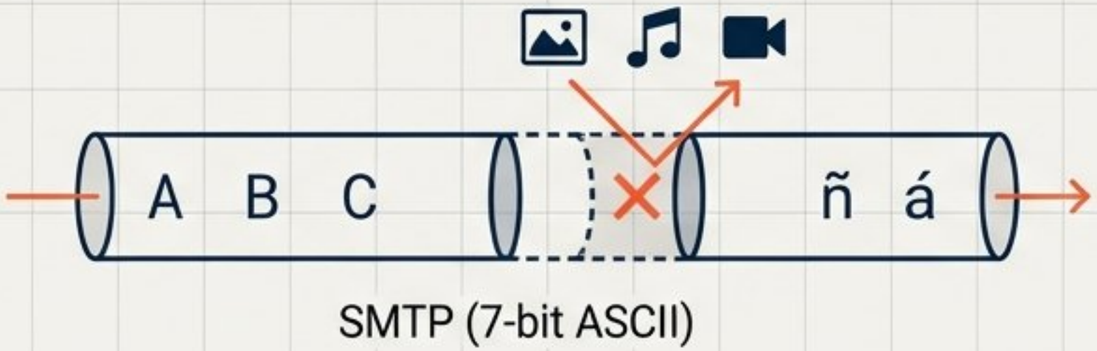
Comparativa de Copias (CC / BCC)

CC (Carbon Copy): Visible para todos.
BCC / CCO (Blind Carbon Copy): Invisible para los demás destinatarios (Privacidad).

Technical Manual meets Swiss Design. Reference Schematic: <IMAGE_0>

MIME: Rompiendo las Barreras del Texto

El Problema



SMTP (7-bit ASCII)

SMTP original solo soporta texto inglés básico.

La Solución: MIME

Multipurpose Internet Mail Extensions

Inicialmente aparecen 5 nuevas cabeceras:

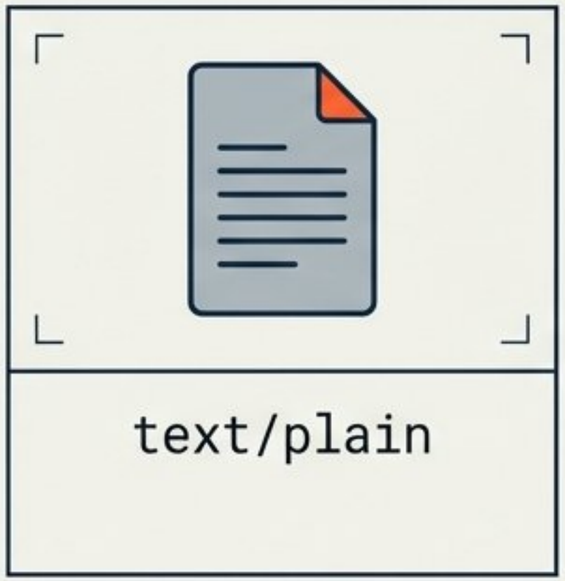
MIME-Version: `1.0` ⟶ Permite especificar el tipo de contenido.
Content-Type: `text/plain; image/gif; video/mpeg; ...`
`(text/plain; image/gif; video/mpeg; ...)`
Content-Transfer-Encoding: `7bit, quoted printable o base64`
(esquemas de codificación: 7bit, quoted printable o base64, 8bit o binary en función del MTA)
Content-Id: `<id_unico>` ⟶ (Para referenciar una parte del mensaje)
Content-Description: `descripción_opcional`

Permite mensajes multipart (con delimitadores o boundaries).

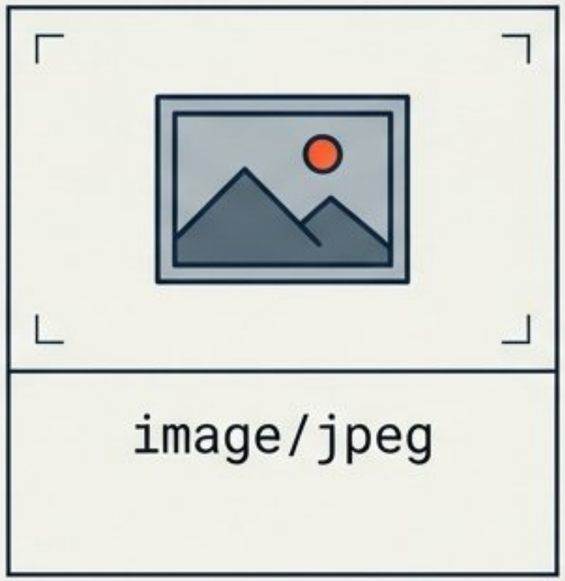
Technical Manual meets Swiss Design. Reference Schematic: <IMAGE_0>

Tipos de Contenido y Codificación MIME

CONTENT-TYPES



`text/plain`



`image/jpeg`

`audio/mp3`

`multipart/mixed`

→ Fundamental para adjuntos

CODIFICACIÓN (ENCODING)

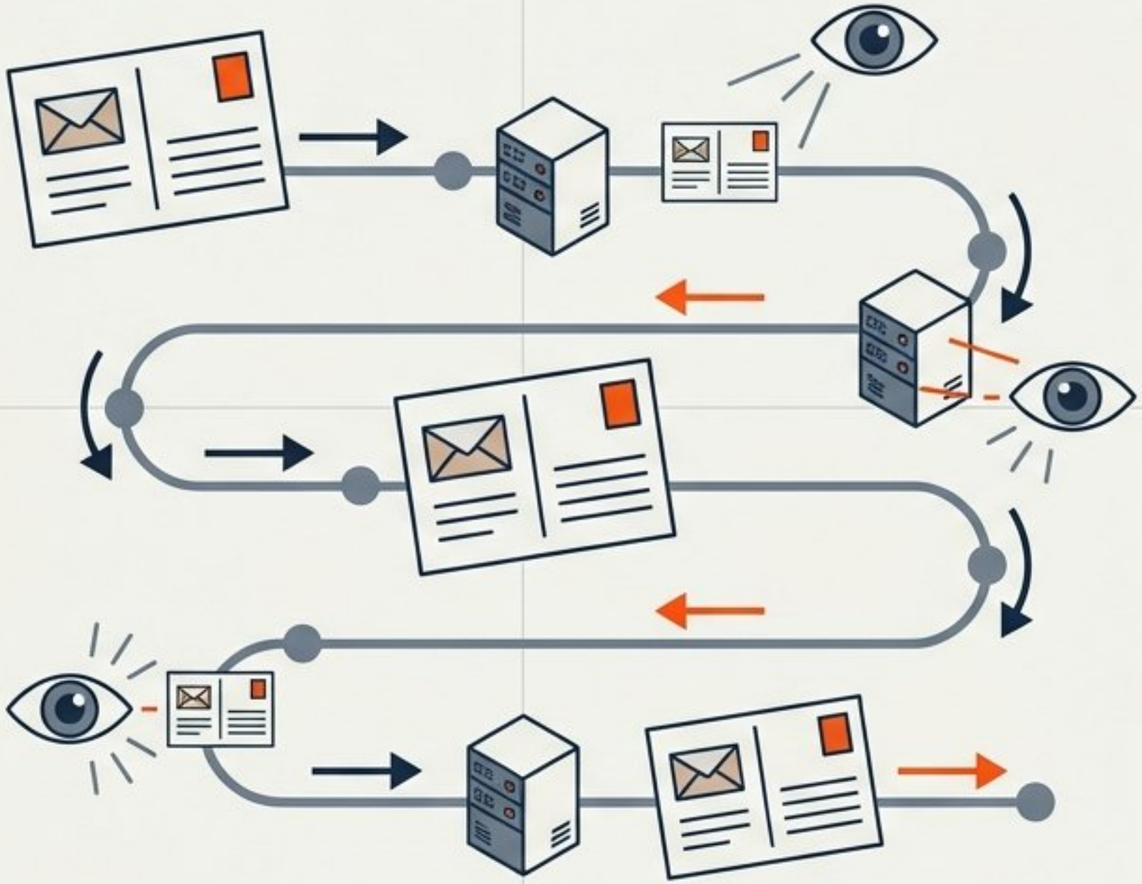
Base64

Convierte binarios en texto ASCII seguro para transporte.

Quoted-Printable

Para texto con caracteres especiales puntuales (tildes).

La Necesidad de Seguridad: Un Sistema Abierto



Por defecto, el email es público como una postal.

Tríada de Seguridad (CIA)

Technical Manual meets Swiss Design.
Reference Schematic: <IMAGE_0>

Criptografía: Firma Digital vs. Cifrado

Firma Digital (Autenticación + Integridad)

Se captura el cuerpo del mensaje → Se calcula el valor de hash del mensaje → Se recupera la clave privada del remitente → Se cifra el valor de hash con la clave privada del remitente → Se anexa el valor de hash cifrado → Se envía el mensaje

Usa **Clave Privada del Remitente**. Garantiza origen y que no hubo cambios.

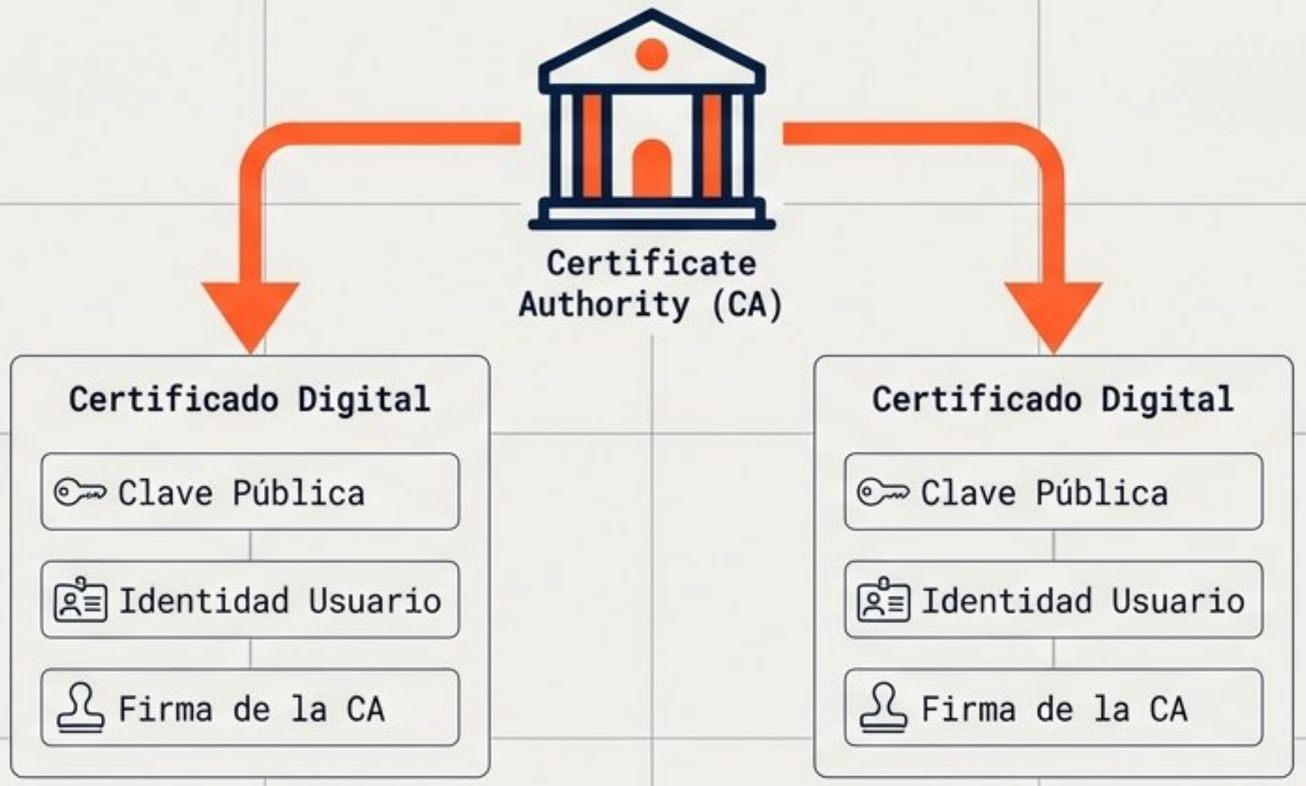
Cifrado (Confidencialidad)

Se captura el cuerpo del mensaje → Se recupera la clave pública del destinatario → Se cifra el mensaje con la clave pública del destinatario → Se envía el mensaje cifrado → Se descifra el mensaje con la clave privada del destinatario

Usa Clave Pública del Destinatario. Garantiza privacidad total.

Technical Manual meets Swiss Design.
Reference Schematic: <IMAGE_0>

Certificados Digitales: La Cadena de Confianza



Autoridad de Certificación (CA): Entidad de confianza (ej: FNMT, Verisign) que valida las identidades.
Función: Vincula una clave pública a una persona real.

Para firmar y cifrar, ambos extremos necesitan certificados válidos.

Resumen y Perspectiva Técnica

Balance del Servicio

Ventajas

- Asíncrono
- Universal
- Bajo Coste

Desventajas

- Phishing
- Malware
- Sin garantía de recepción nativa

Llamada a la Acción: Análisis de Tráfico

Technical Manual meets Swiss Design.
Reference Schematic: <IMAGE_8> & <IMAGE_1> & <IMAGE_2>