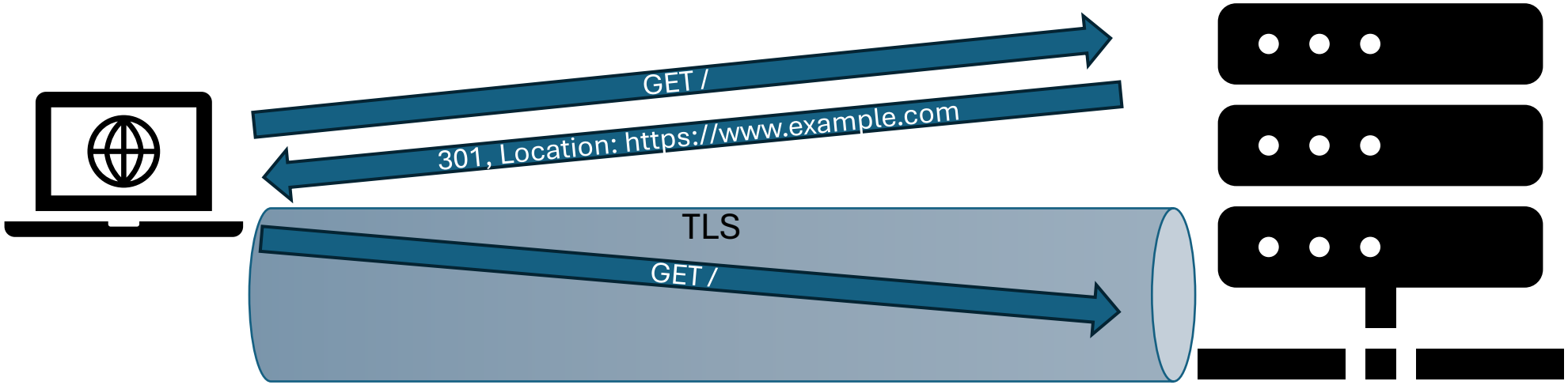
API Keys and Privacy

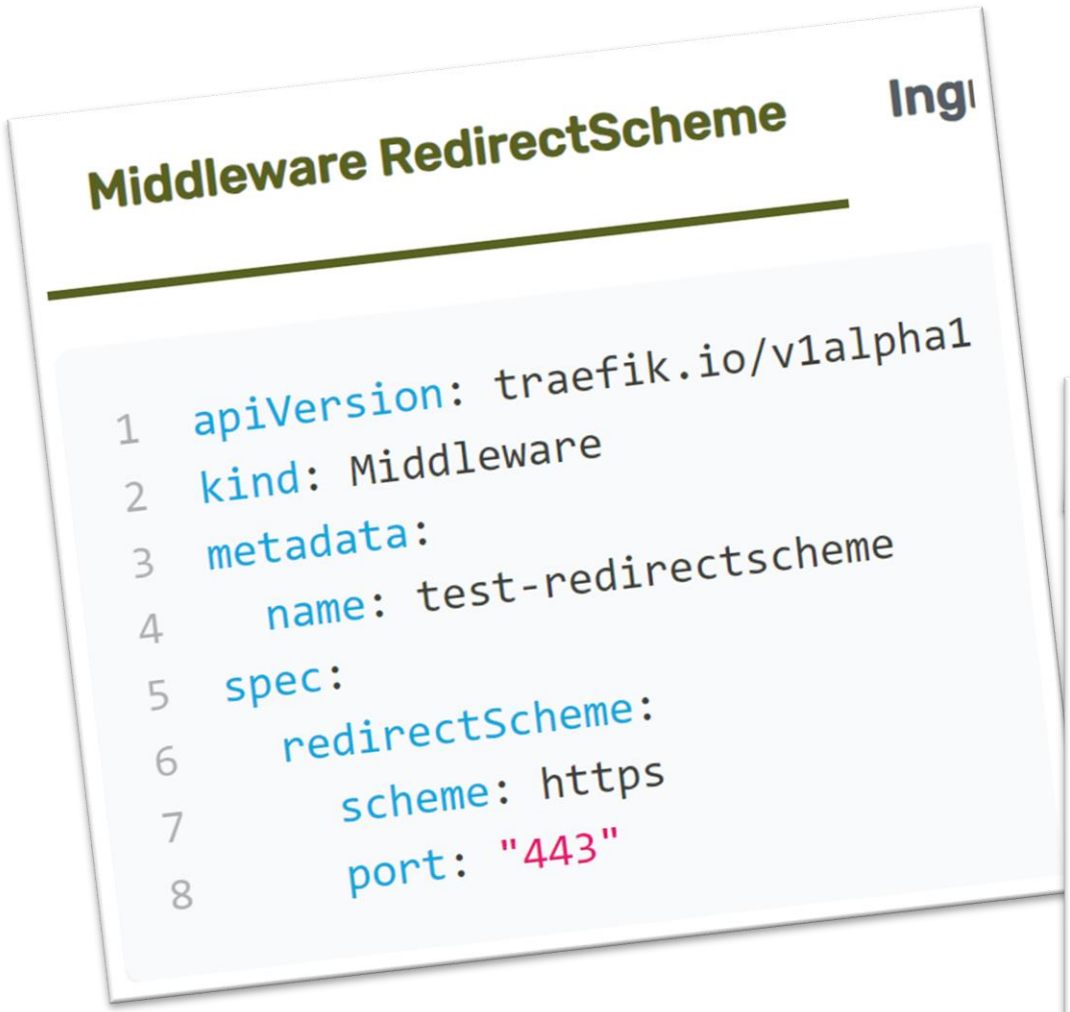
draft-rsalz-httpapi-privacy-00

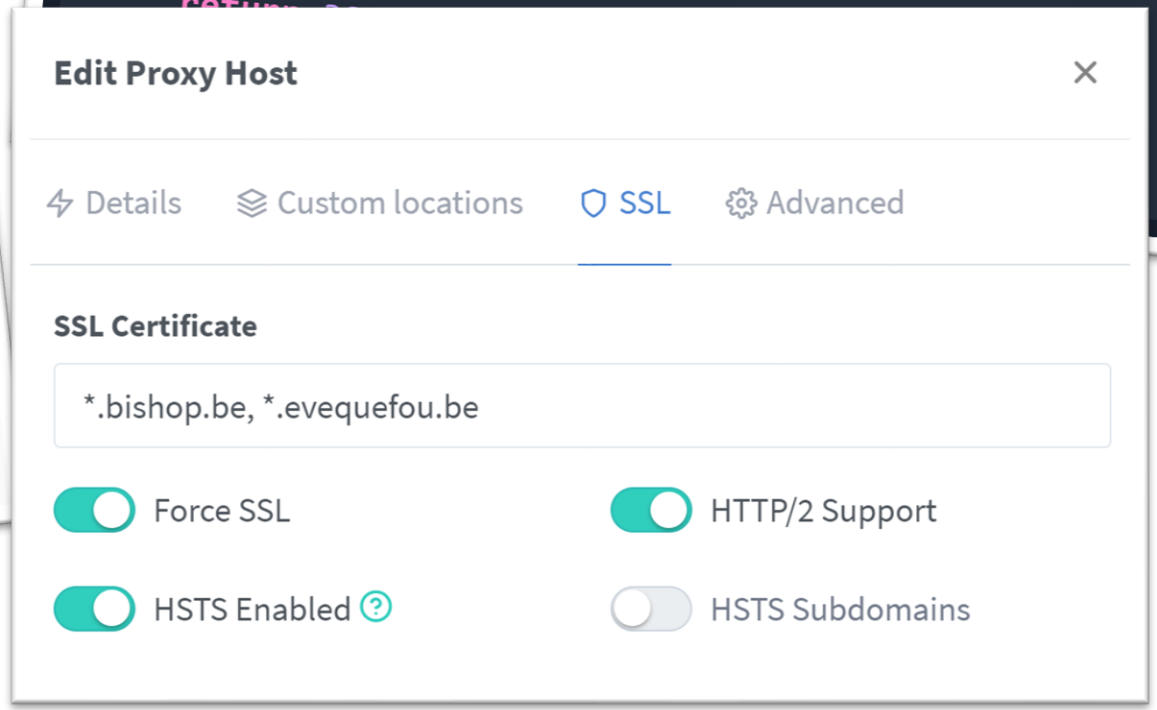
Rich Salz, **Mike Bishop**, Marius Kleidl

Look familiar?

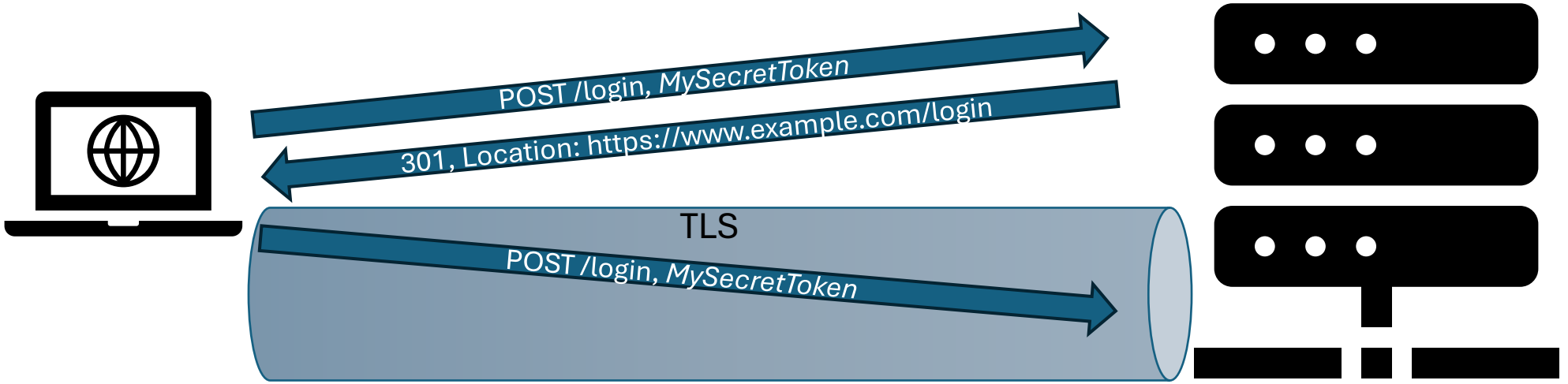


This is ubiquitous!

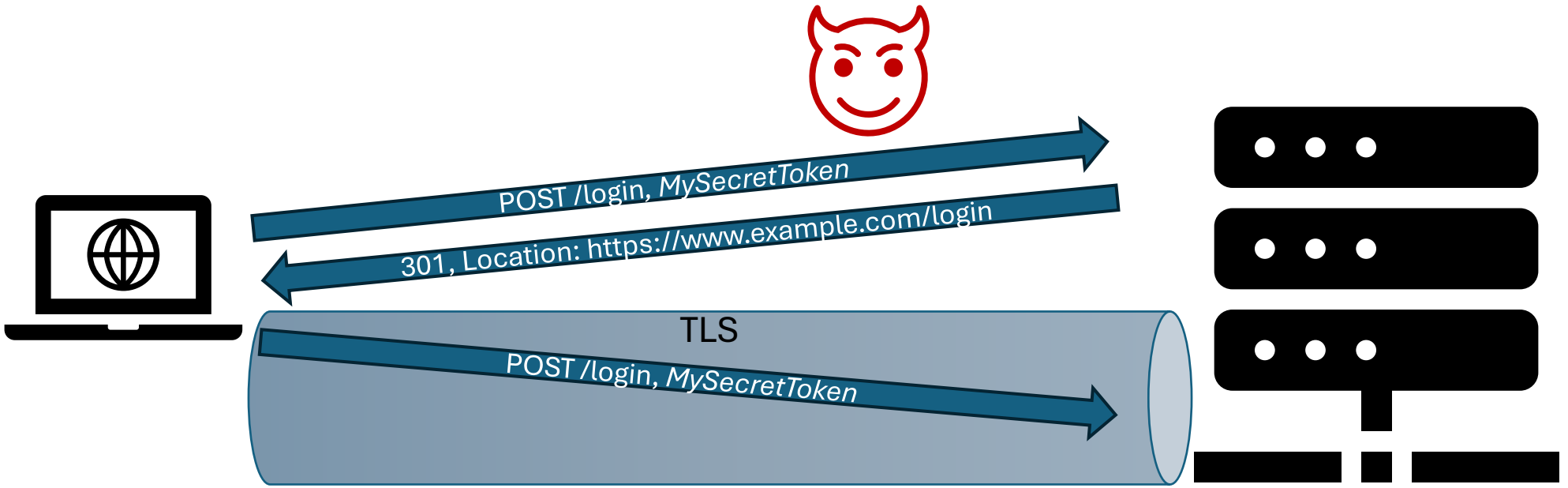




Is this different?



Is this different?



APIs with credentials should never be unencrypted

How do we stop it?

Servers

- Just don’t listen on port 80!
- …but if you can’t:
  - Use HSTS headers and HTTPS records
  - Revoke disclosed credentials

API Clients

- TLS-only by default
  - Require explicit opt-in to use plain-text
- Do HTTPS resolution
- Implement HSTS

Current state

- I-D published, some feedback
- Call for Adoption issued
  - Adopted