

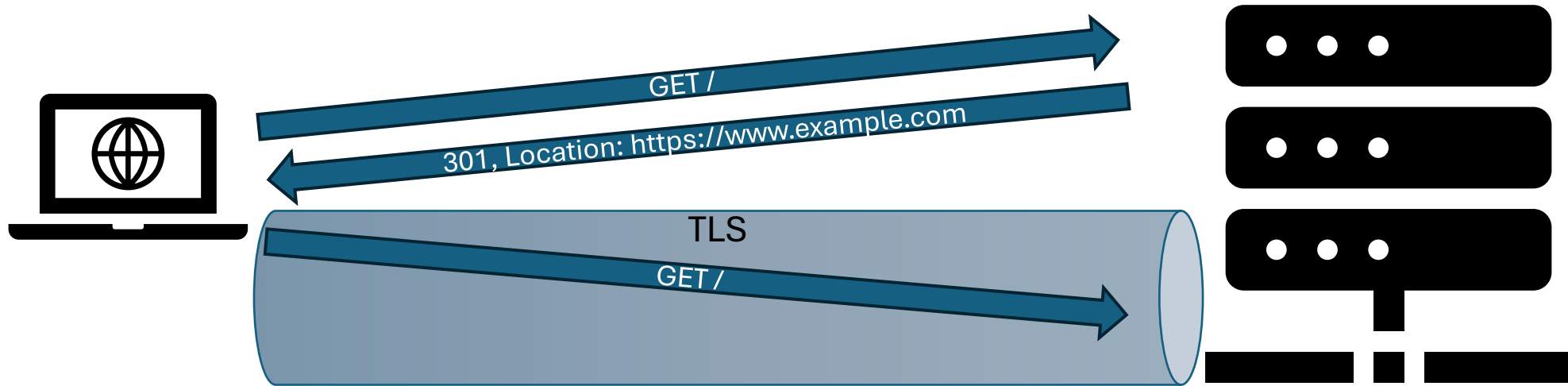


# API Keys and Privacy

draft-rsalz-httpapi-privacy-00

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

# Look familiar?



# This is ubiquitous!

## Middleware RedirectScheme

Ingl

```
1 apiVersion: traefik.io/v1alpha1
2 kind: Middleware
3 metadata:
4   name: test-redirectscheme
5 spec:
6   redirectScheme:
7     scheme: https
8     port: "443"
```

To create a single catch-all HTTP block which will redirect the visitors to the site, open the Nginx configuration file and make the following changes

```
server {
  listen 80 default_server;
  listen [::]:80 default_server;
  server_name _;
  return 301 https://$host$request_uri;
```

### Edit Proxy Host

Details Custom locations **SSL** Advanced

#### SSL Certificate

\*.bishop.be, \*.evequefou.be

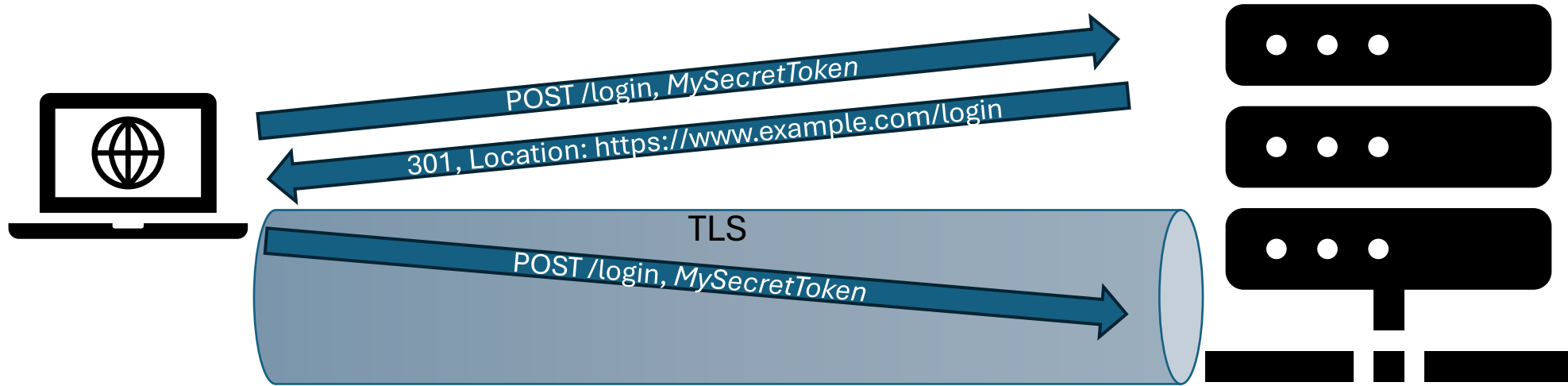
Force SSL

HTTP/2 Support

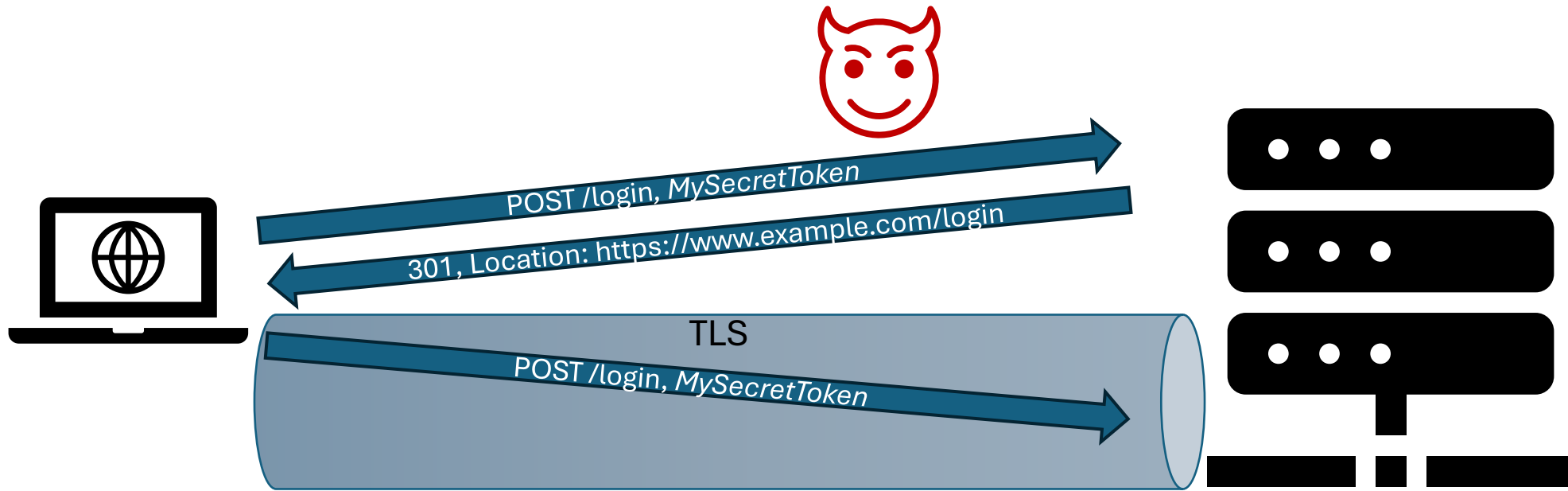
HSTS Enabled ?

HSTS Subdomains

# 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