TOTP Secure Enrollment

(Time-Based One Time Password)

HotRFC Lightning Talk

Brian Contario — Silent Sector

Draft:

https://datatracker.ietf.org/doc/draft-contario-totp-secure-enrollment/

Goal:

Stop leaking the non-expiring TOTP secret during enrollment

Legacy TOTP QR code: Secret Key in Plaintext

- The BASE32 secret is inside the QR and never expires.
- Contains not just the secret, but also the username and what it is for.

QR contents (fully decoded otpauth URI):

```
otpauth://totp/ExampleApp:human@domain.com?
secret=JBSWY3DPEHPK3PXP&
issuer=ExampleCorp&digits=6&period=30
```

Real World Security Failure

- Screenshots sent to enroll remote users via ticketing, chat, email, SMS-MMS systems live indefinitely.
- Printed QR codes for “backups” get discovered.
- Laptop screens in public can get photographed.
- Users copy/paste text strings into notes or cloud drives (not realizing they are shared secrets).
- Breaches/leaks later from “harvest-now, ~~decrypt~~-later” risk.

search

Secure Enrollment QR: One-time use URL

- Replace secret key value with HTTPS URL and a nonce (one time token).
- No TOTP key in the QR; nothing reusable to exfiltrate.

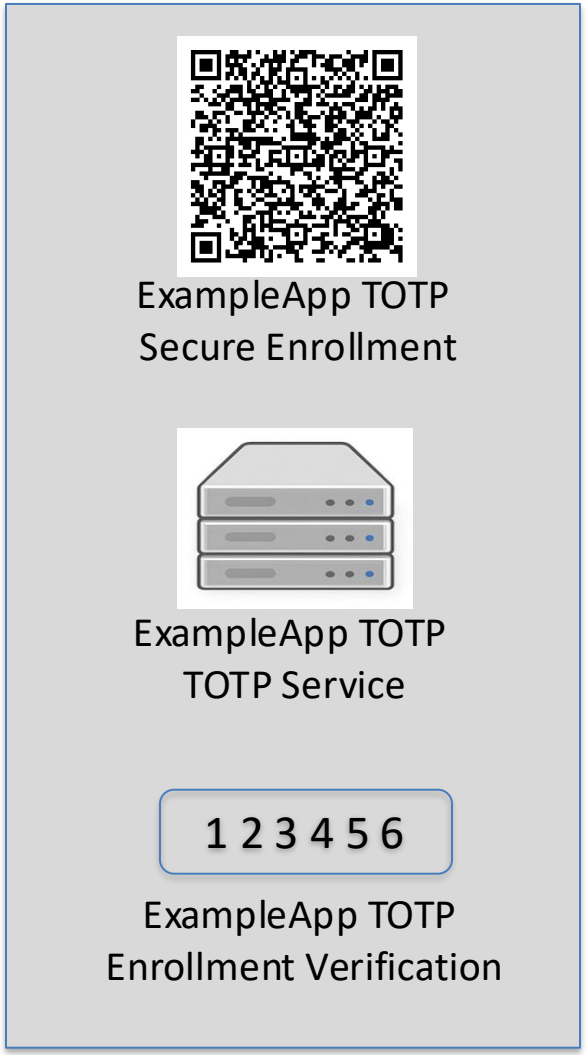
QR contents (decoded secure otpauth URI):

```
otpauth://totp/?secret=https%3A%2F%2Fexamplecorp.com
%2Fapi%2Fenrollmfa%2F16062671560671769238465892
```

HTTPS URL (decoded from “secret” value):

```
https://examplecorp.com/api/enrollmfa/16062671560671769238465892
```

Confidential Key Exchange over HTTPS



1) Scan Secure QR code

```
otpauth://totp/?secret=https%3A%2F%2Fexamplecorp.com
%2Fapi%2Fenrollmfa%2F160626715606717692384658 92
```

2) HTTPS TLS POST + Enrollment Metadata

```
https://examplecorp.com/api/enrollmfa/
160626715606717692384658 92
```

3) HTTPS TLS Response

```
otpauth://totp/ExampleApp:human@domain.com?secret=JB
SWY3DPEHPK3PXP&issuer=ExampleCorp&digits=6&period=30
```

4) Type TOTP One Time Code

```
123456
```

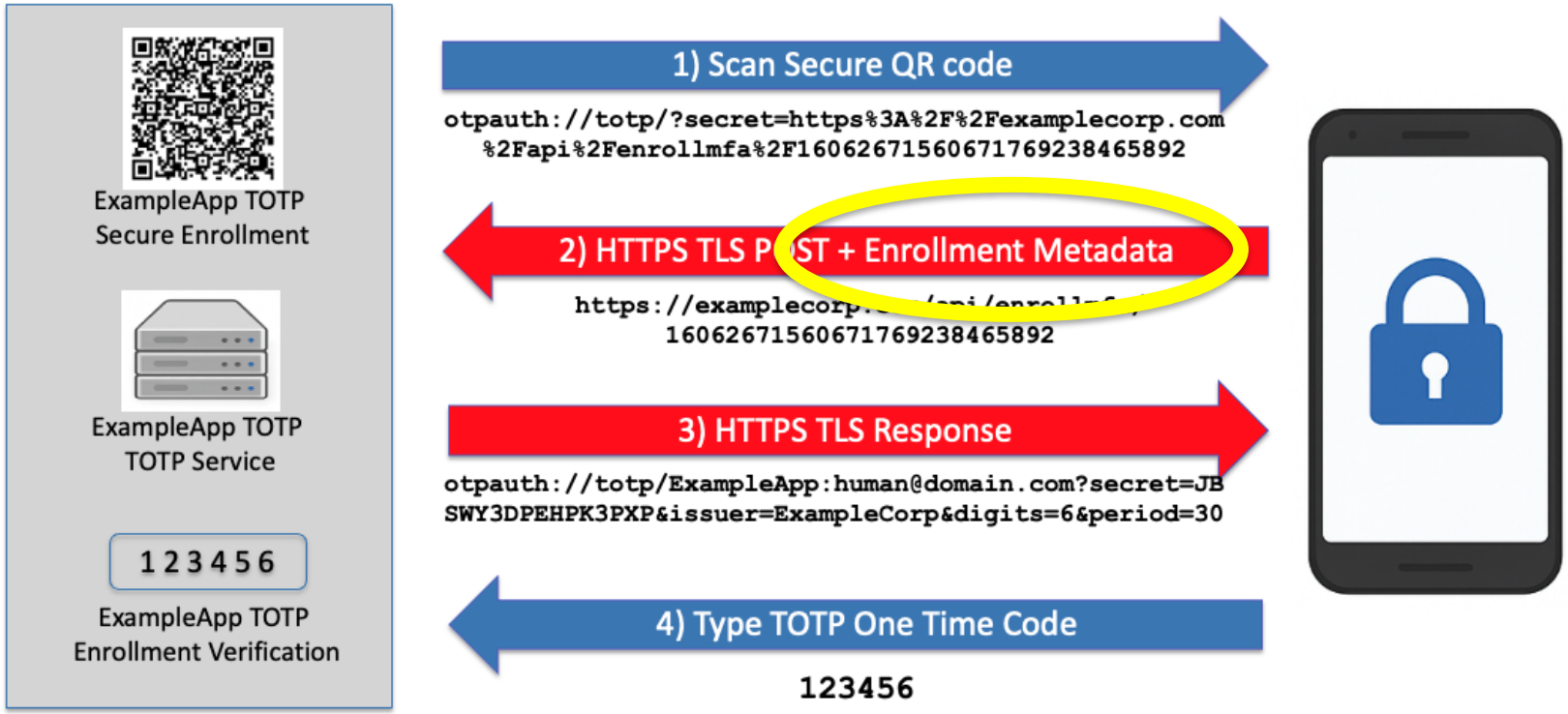
- Same UX; One-time redeem; short nonce TTL; server avoids logging the secret.

Security Properties / What This Solves

- Prevents recovery of the TOTP key from old QR images or screenshots.
- Downgrade Prevention: legacy QR can be disabled by policy.
- Drop-in Code: utilizes a standard otpauth URI for the enrolled key.

Bottom Line: We are sending the original otpauth:// URI content over TLS instead of in a QR code.

New Functionality – Enrollment Metadata



- Eliminates blind enrollment - TOTP Service can finally know what device/app was enrolled
- Allow TOTP prompt to offer hints:
  - “Enter 6 digit code from Microogle Authenticator on your MegaPhone 17”
  - “Enter 6 digit code from PassWarden password manager”

Call to Action

- Looking for implementers (authenticator apps + TOTP servers).

- Draft: https://datatracker.ietf.org/doc/draft-contario-totp-secure-enrollment/
- Authenticator PR: https://github.com/silentbrianc/Aegis/pull/1
- Server PR: https://github.com/silentbrianc/aspnetcore/pull/2

- Catch me after HotRFC / email: bcontario@silentsector.com