TM913 – Two-Factor Authentication (Security Use Case)

Use Story (brief):

As a user, I want to enable two-factor authentication (2FA) so that my account is more secure against unauthorized access.

Actors: User, MenuMap System, Email/SMS Service

Preconditions:

1. User is registered and logged in.

2. User has a valid email/phone number registered.

Description:

1. User navigates to “Security Settings” → “Enable 2FA.”

2. System generates a secret and provides setup (QR code for authenticator app or SMS code).

3. User verifies by entering a one-time code.

4. System stores 2FA setting as active.

5. On next login, after entering password, system prompts for OTP.

6. Access granted only after successful OTP validation.

Postconditions:

- User account has 2FA enabled.

- Login flow now requires an additional authentication factor.

NFRs:

- OTP expires in 60 seconds.

- Must follow OWASP MFA guidelines.

- Recovery codes available in case of device loss.