Test Case: MFA Soft Token (TOTP) Logic With Provided Secret

Preconditions:
- Mint account is configured for 'soft token' MFA (e.g. authenticator app/TOTP).
- The TOTP secret is available.
- Chrome WebDriver and dependencies set up.

Steps:
1. Launch Chrome WebDriver.
2. Call sign_in() with:
   - Valid email and password
   - driver instance
   - mfa_method = constants.MFA_VIA_SOFT_TOKEN
   - mfa_token = correct TOTP secret shared with oathtool.generate_otp
   - mfa_input_callback = None
   - wait_for_sync = False
3. Observe the flow: oathtool generates TOTP code, it is entered and submitted automatically.
4. sign_in() completes successfully.

Expected Result:
- TOTP (soft token) code is generated via oathtool and submitted automatically.
- If the TOTP setup is correct, login proceeds without further manual steps.

---Extra Details---
Filename: signIn.py
Description: Tests that the soft token (TOTP) MFA logic is handled correctly and oathtool generated code is used. Ensures no ma
Score: 87%
Alignment: 78%
Validation Notes: Accurately tests soft token scenario. Account must be configured for this MFA method. Validates oathtool usage