Integration verification checklist

Before submitting your information into the online form, use this checklist to ensure you collect all the necessary information

1. Company name
2. Product name
3. Industry/product category (select all that apply)
    - Blockchain and cryptocurrencies
    - Browser
    - Cloud services
    - Communications
    - Developer tools
    - Domains
    - Education
    - Financial services
    - Gaming
    - Government
    - Hardware security module
    - Healthcare
    - Identity management
    - Internet of things
    - Legal
    - Media and entertainment
    - Productivity
    - Public key infrastructure
    - Retail
    - Security
    - Transportation
    - Utilities
    - Other
4. Support protocols (select all that apply)
    - Challenge response
    - FIDO2/WebAuthn
    - One-time password (Yubico OTP)
    - One-time password (Yubico OTP - custom configuration required)
    - One-time password (TOTP)
    - One-time password (HOTP)
    - OpenPGP
    - Smart Card (PIV)
    - Universal 2nd factor (U2F)
5. Can an end user register a YubiKey with your product?
    - Yes
    - No
6. Can an admin register a YubiKey on behalf of an end-user?
    - Yes

    - No
7. Can an end user authenticate to your product using a registered YubiKey?
    - Yes
    - No
8. Will an end-user's login attempt be rejected if authenticating with an unregistered YubiKey?
    - Yes
    - No
9. Can an end-user register multiple YubiKeys with your product? (recommended)
    - Yes
    - No
10. How many YubiKeys can be registered?
    - Enter response
11. Can an end-user unregister or remove a YubiKey after it's been registered?
    - Yes
    - No
12. Can an admin remove a YubiKey on behalf of an end-user?
    - Yes
    - No
13. How does the end-user initiate this request?
    - Enter response
14. Can an end-user name or rename a registered YubiKey? (recommended)
    - Yes
    - No
15. Can an end-user prevent the same YubiKey from being registered again?
    - Yes
    - No
16. Do you also have a PIV implementation?
    - Yes
    - No
17. Can an admin provision and load a certificate onto the YubiKey?
    - Yes
    - No
18. Can an end-user provision and load a certificate onto the YubiKey?
    - Yes
    - No
19. How can certificates be provisioned and loaded onto the YubiKey?
    - Enter response
20. How is the Management Key being set?
    - Enter response
21. Where is the value being stored?
    - Enter response
22. Are any Yubico libraries or APIs being utilized?
    - Yes
    - No
23. If yes: Which libraries are in use (e.g. Yubico minidriver, PIV tool, etc.)?

    - Enter response
24. If no: How is the certificate loaded onto the key?
    - Enter response
25. Can an end-user authenticate with the YubiKey in Smart Card mode?
    - Yes
    - No
26. Does your UI use the correct terminology and Yubico and YubiKey branding?
    - Yes
    - No
27. Is a method for account recovery in place should an end-user lose a registered YubiKey?
    - Yes
    - No