Managing Your FIPS YubiKey (WCSC)

The purpose of this document is to help you understand and choose between WidePoint managing your YubiKey or your company managing your YubiKey. This is a choice that your company should make as a whole, please bring this document to your Security/IT Teams.

Note: Printed copies of this document may not contain the most recent updates.

WidePoint Managed or Self Managed FIPS YubiKey

Before installing any certificates onto your FIPS YubiKey you and your company must decide if they want to manage your YubiKeys information yourselves, or if you would like Widepoint to manage the YubiKey. The decision should be made for your entire company, please reach out to your Seecurity and IT teams and consult the decision with them.

WidePoint offers two options for YubiKeys: Self Managed and Widepoint Managed. The 9B value and PUK can be managed by WidePoint or your company, but you will always need to manage your own PIN and encryption certificate.

Important Note: YOU MUST SPEAK TO YOUR COMPANY REGARDING THIS. Once this choice has been made it needs be stuck to; if this decision is changed in the future, it will involve deleting and having to repurchase all certificates. This decision should be company-wide, we recommend having your YubiKey be Widepoint managed if your company does not already have a PKI team.

- **Self Managed**
  You and your company will need to manage your 9B Value and PUK. These codes cannot be lost; If either value is lost you will not be able to renew certificates in the future. If the PUK value is lost you will not be able to change the PIN of the YubiKey. You will not be able to change your PIN using the WidePoint YubiKeySolution application if you choose this option.

  You and your company will need to use the Yubico Authenticator application to setup the 9B value and the PUK. Widepoint will not assist with the management or setup of your YubiKey if you choose this option.

  The choice to Self-Manage your YubiKey should be made if any of the following statements are true.

  - YubiKey currently has certificates on it that need to be kept.
    - Widepoint requires the 9A and 9B slots to be empty for Medium Token Assurance Certificates and Medium Hardware Assurance Certificates; The 9C slot will need to be empty if you are purchasing a Code Signing Certificate.
  - YubiKey will be used for smartcard Logon.

  - YubiKey will be used for any PIV functions in the future, outside of Widepoint ECA Certificates.

- **Widepoint Managed**
  WidePoint will manage your 9B Value and PUK for you. This will allow you to use the WidePoint YubiKeySolution application to change your PIN. Your company will not need to track any details about your YubiKey; The PIN and the encryption certificate will still need to be tracked by the End User. Only the End User is allowed to be in possession of the YubiKey, the PIN, and the encryption certificate.

  If none of the 3 statements in the above **Self Managed** section are true, then use the below statements about using a WidePoint Managed YubiKey to help decide between the two options.

  - Only requires the End User to hold onto their PIN and Encryption Certificate. Takes the duty of information tracking off of your company. Easier for small companies who do not have a process in place for tracking this kind of information.
  - Allows End Users to use the Widepoint YubiKeySolution application to change their PIN. Our application does not have the ability to delete your certificates or accidentally reset your YubiKey. If you choose the Self Managed option then you would need to use the Yubico YubiKey Manager application to do PIN changes, and this application allows the deletion of certificates.

If you company has any questions regarding the management of your YubiKey that is not answered in this document, please contact wcsc.helpdesk@widepoint.com.