Vertraulichkeit und Datenschutz mit YubiKey Token

Der YubiKey ist ein Hardware-Authentifizierungsgerät von Yubico. Sie können sich das Gerät als einen winzigen Safe vorstellen, auf dem Anmeldeinformationen sicher und unabhängig von einem Computer gespeichert werden können. Es gibt ihn in den verschiedensten Größen: Von einem Token, der groß genug ist, um am Schlüsselbund getragen zu werden, bis hin zu den kleinsten Modellen, die kaum noch aus dem Gerät herausragen, in dessen USB-Anschluss sie eingesteckt sind. Der YubiKey benötigt weder eine Batterie noch Software, die auf dem Host-Gerät installiert werden müsste. Stecken Sie ihn einfach in einen USB-Port oder verbinden Sie ihn via NFC und schon sind Sie startklar. .

Wie können Sie conpal LAN Crypt zusammen mit MFA nutzen?

conpal LAN Crypt ist eine client-seitige Verschlüsselungslösung, die Verschlüsselung auf Dateiebene bietet. Die leistungsstarke Schlüssel- und Richtlinienverwaltung unterstützt Daten mit unterschiedlichen Schlüsseln für geschäftliche, persönliche und gemeinsam genutzte Daten. Schlüssel, die einem bestimmten Benutzer zugewiesen sind, werden mit standardisierter privater Schlüsselkryptographie verschlüsselt. Nur derjenige Nutzer, der über den privaten Schlüssel verfügt, kann auf diese Schlüssel zugreifen, weswegen der Schutz dieses privaten Schlüssels von höchster Wichtigkeit ist. Der YubiKey Token ist dafür ideal: Durch seine Nutzung werden zwei separate Authentifizierungsfaktoren benötigt – Wissen und Besitz – und dadurch das generelle Sicherheitslevel deutlich erhöht.

Admin

Ausrollen des YubiKey

conpal LAN Crypt nutzt Public-Key-Kryptographie zur Sicherung von benutzergebundenen Verschlüsselungsprofilen. Zu diesem Zweck benötigt jeder Benutzer ein Zertifikat zusammen mit dem zugewiesenen öffentlichen/privaten Schlüsselpaar. Das System ist flexibel in Bezug auf die Herkunft der Zertifikate und den Speicherort des privaten Schlüssels des Benutzers.
Zertifikate können von einer externen Zertifizierungsstelle (CA) importiert werden, von der conpal LAN Crypt-Administration als selbstsignierte Zertifikate generiert werden, oder auf dem YubiKey-Token selbst erstellt werden. Was den privaten Schlüssel betriff, so besteht eine Möglichkeit darin, den Schlüssel an einen sicheren Ort zu importieren, der vom System des Endgeräts selbst bereitgestellt wird. Eine andere Möglichkeit ist, den privaten Schlüssel auf einem YubiKey-Token zu speichern. Wenn das Schlüsselpaar auf dem Token selbst generiert wurde, ist die Speicherung des Schlüssels damit erledigt. Wenn das Schlüsselpaar von einem externen System generiert wurde, muss der private Schlüssel des Benutzers in den Token importiert werden. Sobald der private Schlüssel auf dem YubiKey-Token verfügbar ist, kann der Token verwendet werden, um das conpal LAN Crypt-Profil des Benutzers zu entsperren und die Verschlüsselung zu aktivieren.

Client

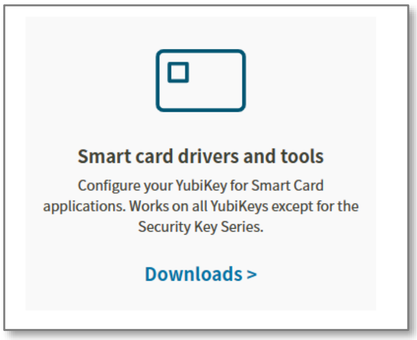
YubiKey Client Software

Zentral verwaltete Token
Wenn der YubiKey-Token zentral registriert ist oder die Schlüssel auf dem Token selbst erstellt wurden, ist der Token für den Endbenutzer einsatzbereit. Die Unterstützung für YubiKey PIV-Token ist bereits in Windows- und MAC-Clients integriert. Es ist nicht notwendig, zusätzliche Software zu installieren, um den Token in conpal LAN Crypt zu verwenden. Stecken Sie den Token einfach in einen USB-Port am Endgerät, wenn Sie dazu aufgefordert werden. Bitte lesen Sie auch weiter unten den Abschnitt über den conpal LAN Crypt Client.

Benutzerverwaltete Token
Der YubiKey-Token kann an den Endbenutzer ausgehändigt werden, ohne dass der private Schlüssel hinterlegt ist. In diesem Fall muss der private Schlüssel des Benutzers in den YubiKey importiert werden, bevor er für die Anmeldung am conpal LAN Crypt Client verwendet werden kann. Dazu muss eine Software von YubiKey auf dem System installiert werden. Bitte folgen Sie den nachstehenden Schritten, um den privaten Schlüssel eines Benutzers in den YubiKey-Token zu importieren.

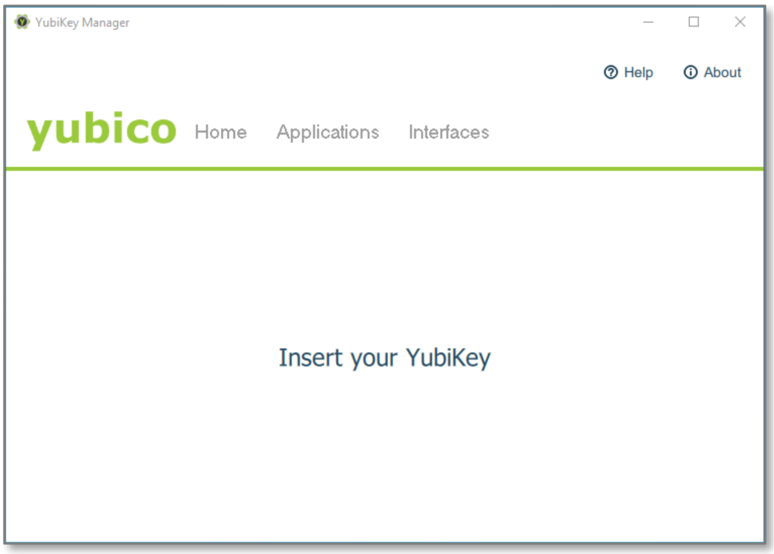
Hinweis:
Die Installationsanweisungen gelten sowohl für Windows- als auch für macOS Geräte.

YubiKey Smart Card Treiber installieren
Der YubiKey Smart Card-Treiber ermöglicht die Zertifikatsregistrierung für Benutzer und Administratoren, erlaubt die Verwaltung der YubiKey Smart Card-PIN und unterstützt die Smart Card-Authentifizierung unter Windows. Er wird von der YuiKey Manager Software benötigt, um den Token zu verwalten.



YubiKey Manager installieren

Der YubiKey Manager umfasst sowohl eine grafische Benutzeroberfläche als auch ein Befehlszeilen-Tool zur Erstellung von PIN-Unlock Keys (PUK) auf YubiKey-Geräten für Kunden, die einen PUK benötigen. Er wird auch verwendet, um den privaten Schlüssel des Benutzers in den Token zu importieren.
Starten Sie den YubiKey Manager und stecken Sie den Token in einen lokalen USB-Anschluss.

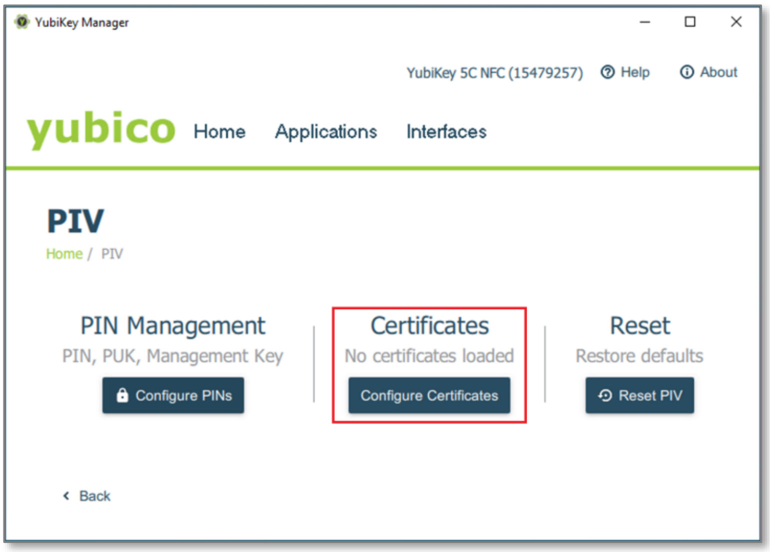


Benutzerschlüssel importieren

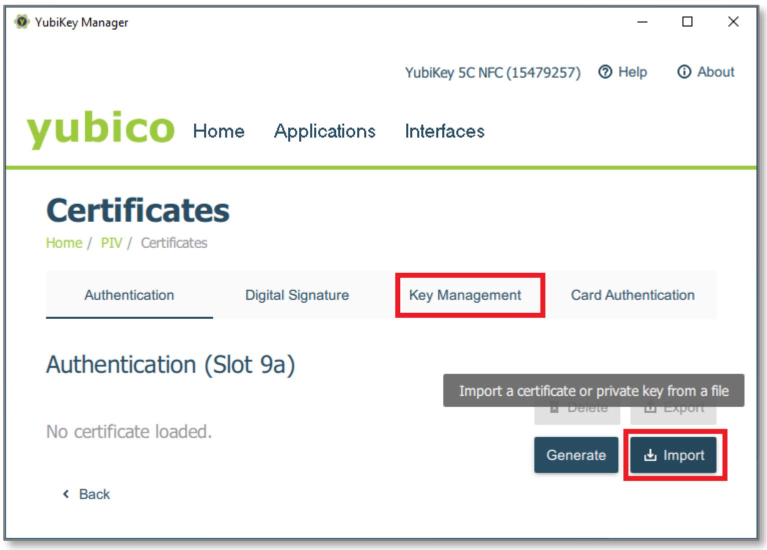
Der nächste Schritt ist der Schlüsselimport. Mit diesem Vorgang wird der Token im Wesentlichen "personalisiert" und an einen bestimmten Benutzer gebunden. Starten Sie den YubiKey Manager und fügen Sie den Token ein.

Navigieren Sie zur Option "**PIV**" im Menü "**Applications**", um das Dialogfeld mit den Smartcard-Optionen aufzurufen.

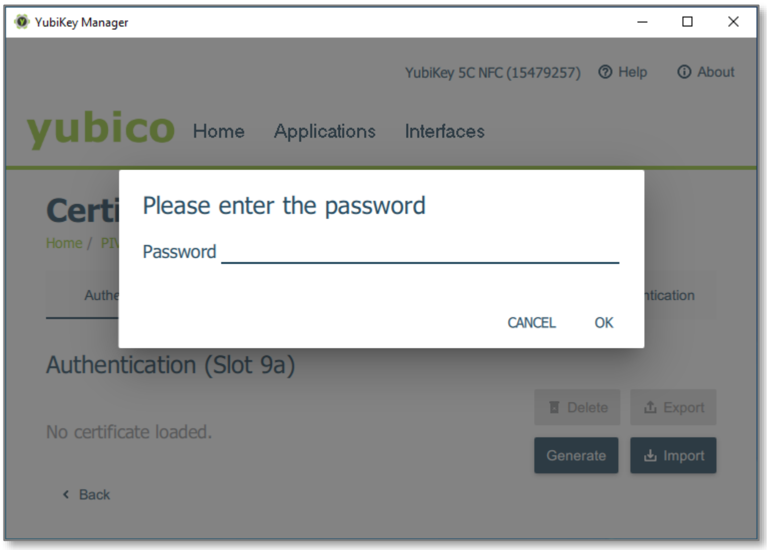
Wählen Sie im PIV-Dialogfeld “Certificates“, um zur Importseite zu gelangen.



Der YubiKey-Token unterstützt vier sogenannte „Slots“ zur Speicherung privater Schlüssel. Jeder Slot hat spezifische Eigenschaften, daher ist es wichtig, den richtigen Slot zu wählen. Für Schlüssel, die mit conpal LAN Crypt verwendet werden sollen, muss der Slot “**Key Management**” verwendet werden. Wählen Sie “**Import**”, um den Vorgang zu starten.



Beim Import werden Sie aufgefordert, den zu importierenden privaten Schlüssel auszuwählen. Wählen Sie die p12-Datei, die sie importieren möchten. In der Regel handelt es sich dabei um die p12-Datei, die Sie von Ihrem conpal LAN Crypt-Administrator erhalten haben. Sie müssen sich gegenüber dem YubiKey-Token authentifizieren (d.h. die PIN und den Verwaltungsschlüssel des Tokens vorlegen), um den Schlüssel importieren zu können.



Nachdem der Importvorgang erfolgreich abgeschlossen wurde, wird ein Bestätigungsdialog angezeigt. Darin werden Ihnen Details zu dem gerade importierten Schlüssel angezeigt, mit denen Sie ihn noch einmal prüfen können.

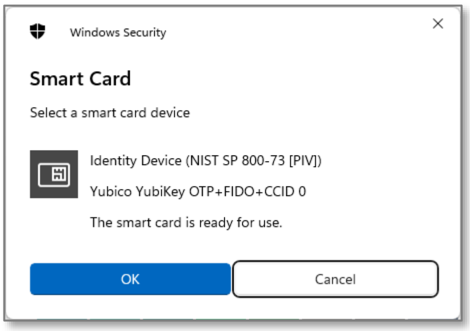
Alles Fertig – der Token kann jetzt in conpal LAN Crypt verwendet werden.

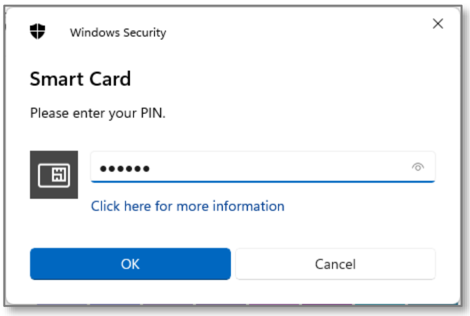
conpal LAN Crypt Client Authentifizierung

Der private Schlüssel des Benutzers wird benötigt, um das Profil zu entschlüsseln bzw. zu entpacken, das dem Benutzer in der conpal LAN Crypt-Verwaltung zugewiesen wurde. Beim Laden des Verschlüsselungsprofils eines Benutzers benötigt der conpal LAN Crypt Client Zugriff auf den privaten Schlüssel des Benutzers. Je nach Speicherort des privaten Schlüssels kann der Benutzer zu einer bestimmten Aktion aufgefordert werden. Im Falle eines YubiKey-Tokens muss der Benutzer den Token einstecken und sich mit seiner privaten PIN gegenüber dem Token authentifizieren, wenn eine Richtlinie geladen oder aktualisiert wurde. Dies ist immer dann der Fall, wenn sich der Benutzer am System anmeldet. Es kann aber auch geschehen, wenn der conpal LAN Crypt-Administrator eine Richtlinienaktualisierung ausgelöst hat.

Token einführen und PIN eingeben

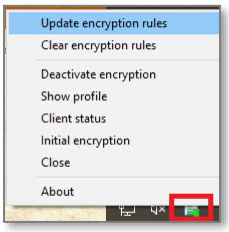
Klicken Sie mit der rechten Maustaste auf das conpal LAN Crypt-Symbol in der Systemablage und wählen Sie “Verschlüsselungsregeln aktualisieren”.





Prüfen der Richtlinie (optional)

Überprüfen Sie das conpal LAN Crypt Symbol in der Systemablage, um zu sehen, ob das Verschlüsselungsprofil erfolgreich geladen wurde. Ein grüner Schlüssel zeigt an, dass alles in Ordnung ist und dass der conpal LAN Crypt Client in der Lage war, das Profil des Benutzers mit dem privaten Schlüssel, der auf seinem YubiKey-Token gespeichert ist, erfolgreich zu entschlüsseln.



Bekannte Einschränkungen

Es gibt keine bekannten Einschränkungen. Alle YubiKey Token der Serie 5 werden unterstützt.