Multi-Factor Authentication and Password Stores with Smart Cards and YubiKeys

James Preston
The Queen's College, University of Oxford
james.preston@queens.ox.ac.uk

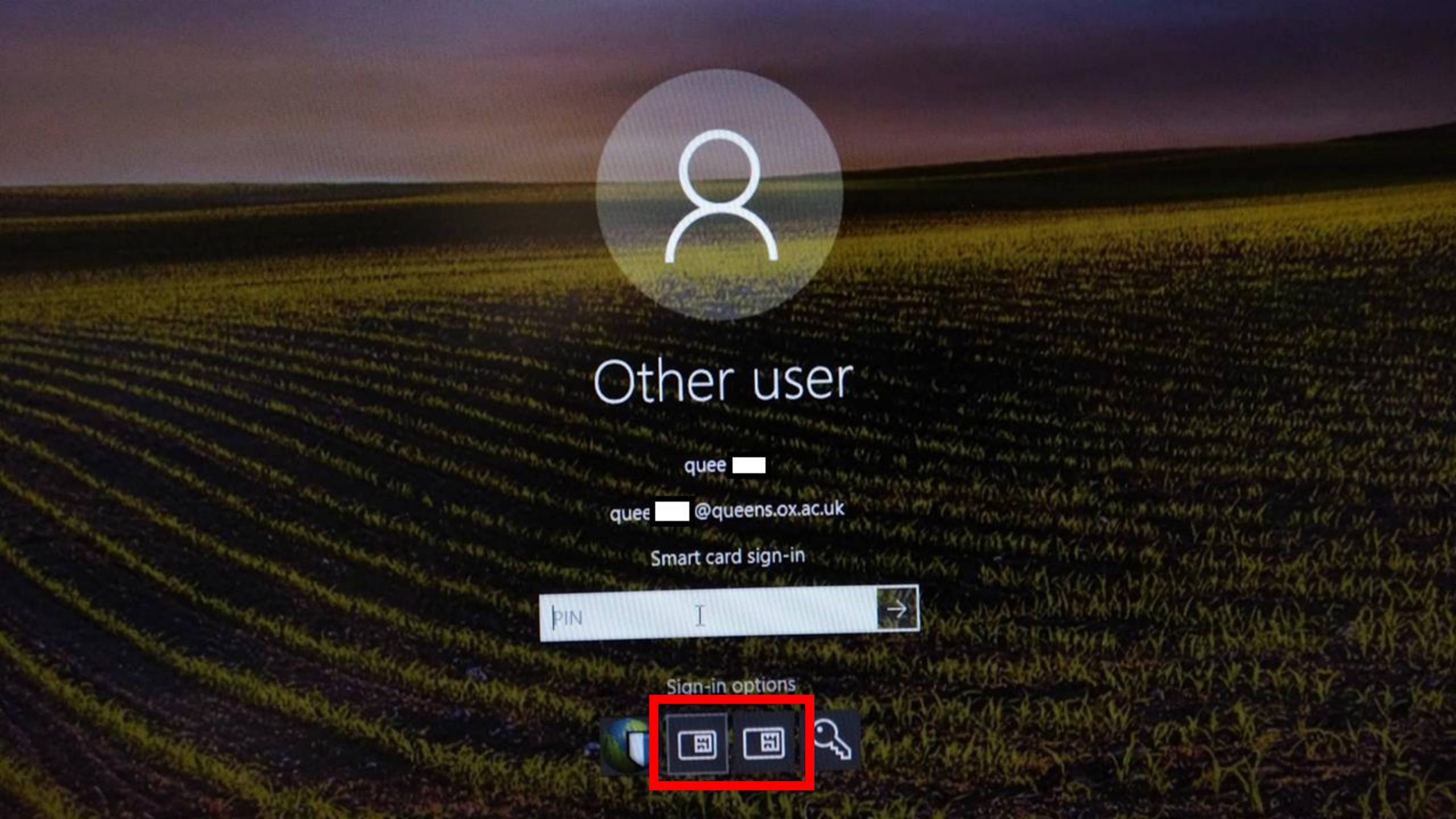
The morning….

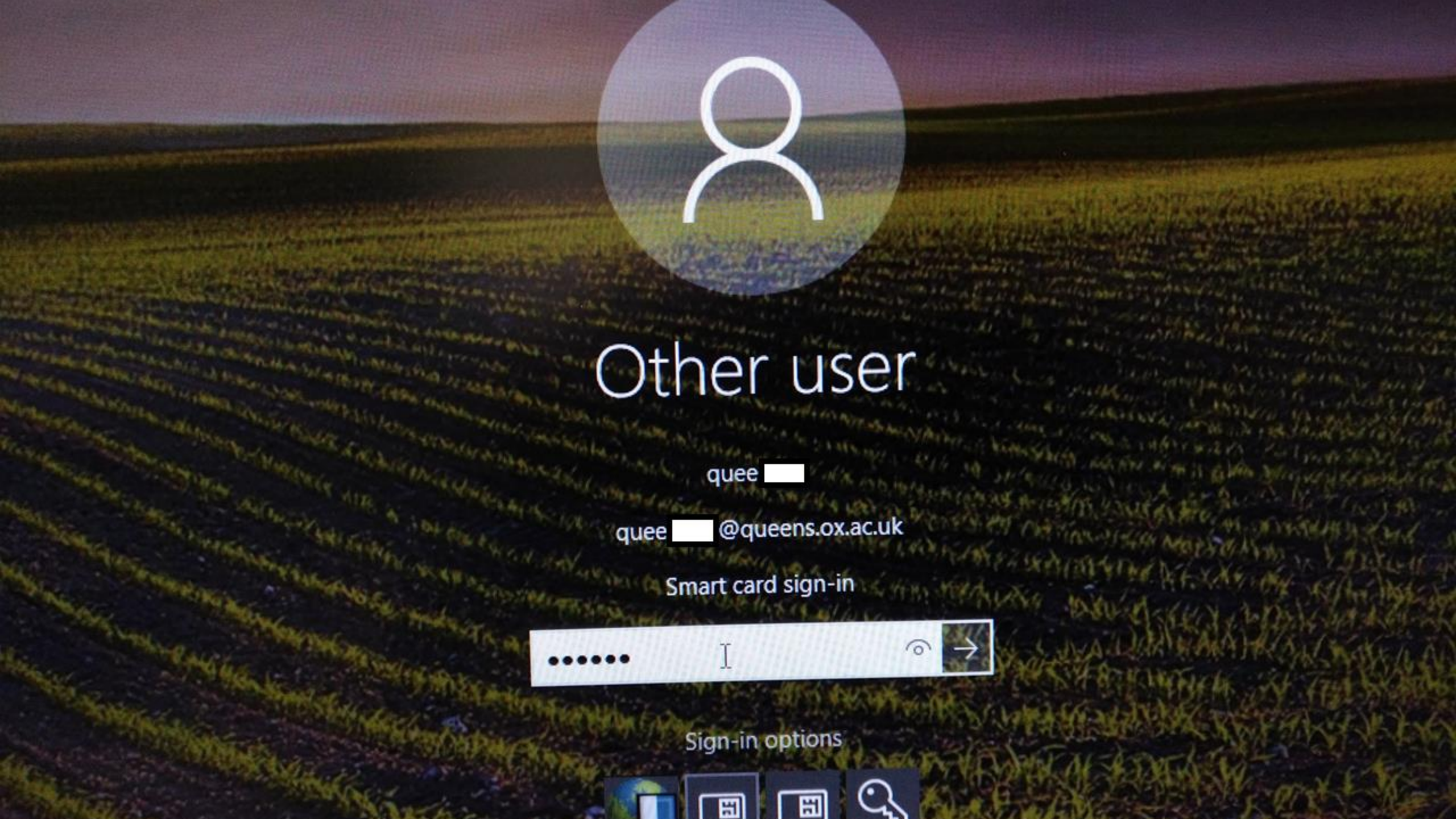

09:05
Wednesday 27 June
UNIFY


Mac Xcode


ThinkPad
OneLink+

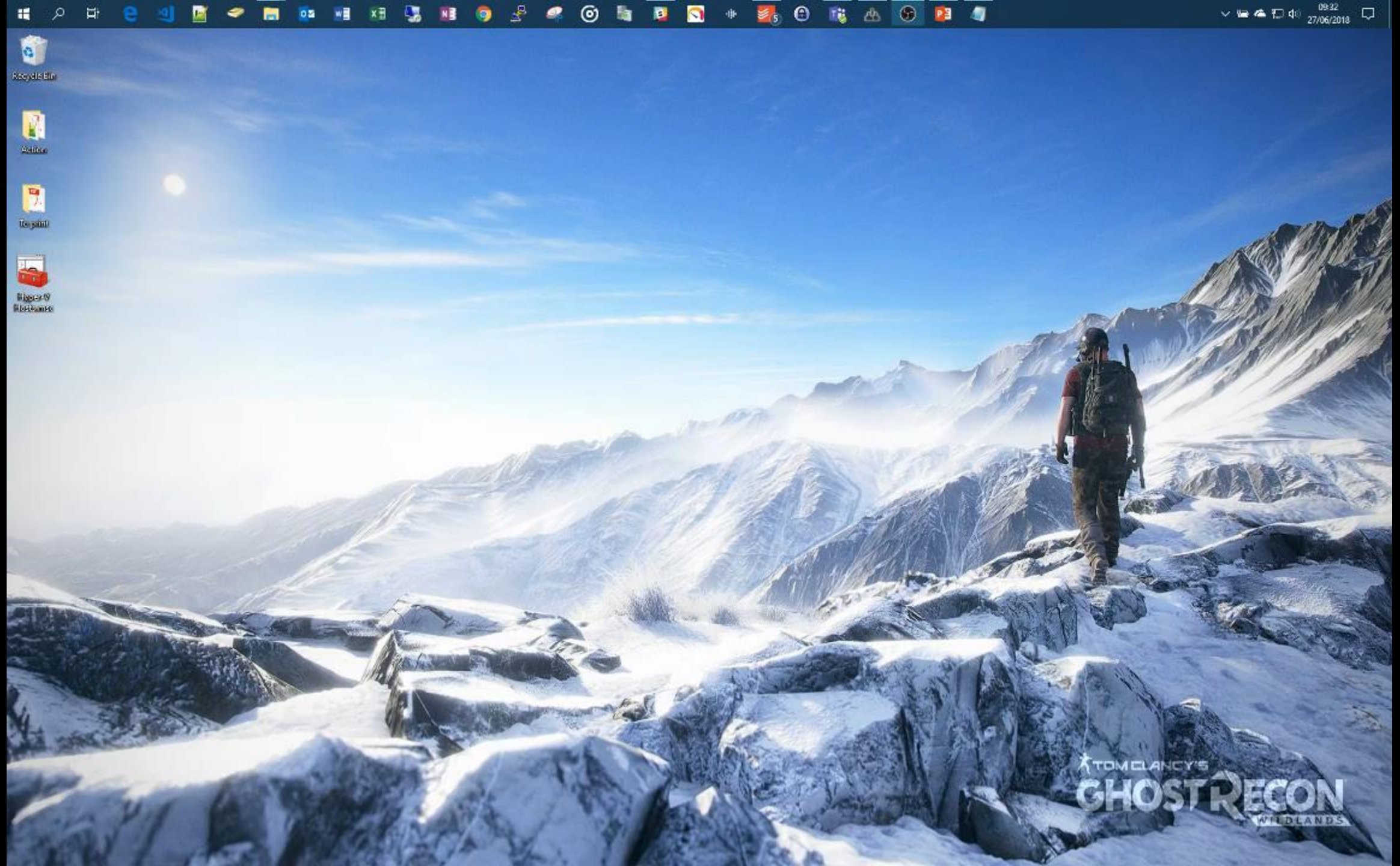

2 Book
WILEY
F-35
OUT: 1A
OUT: 2A

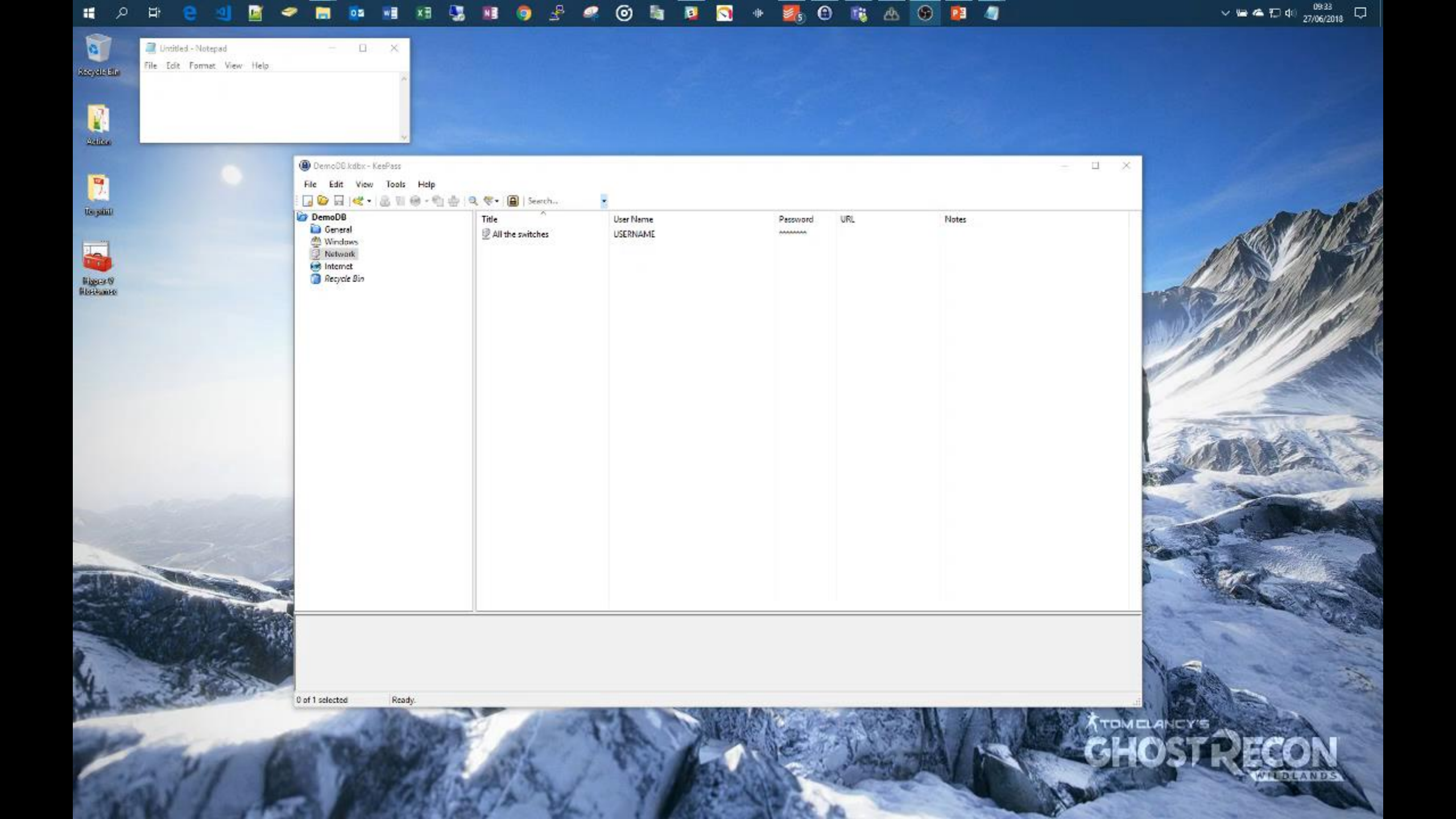

Other user
quee
quee @queens.ox.ac.uk
Smart card sign-in
PIN
Sign-in options


Other user
quee
quee @queens.ox.ac.uk
Smart card sign-in
Sign-in options

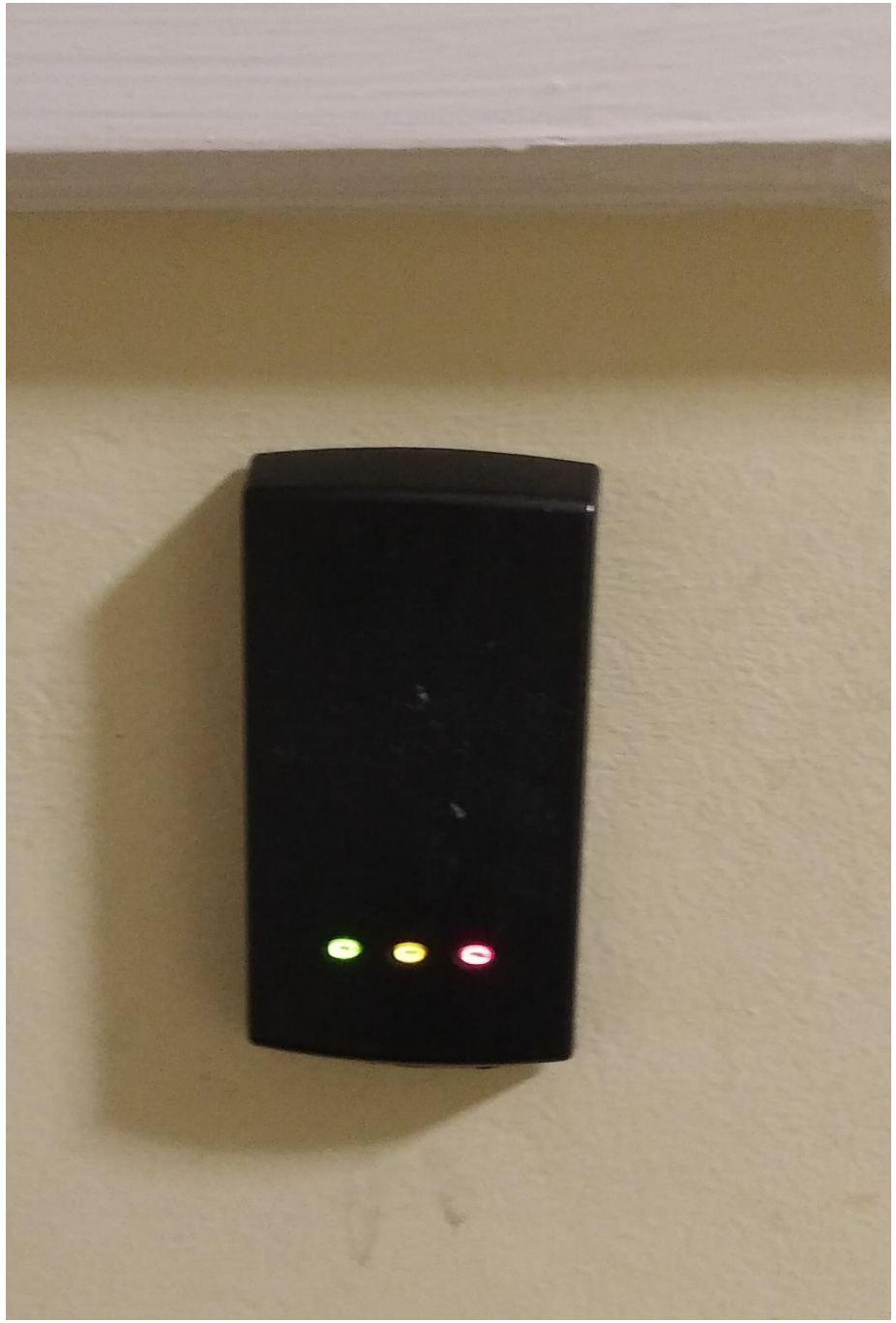

Recycle Bin
Action
To print
Hyper-V Hosts.msc
09:16
27/06/2018


Recycle Bin
Action
To print
Hyper-V Hosts.msc
09:29
27/06/2018


Recycle Bin
Archive
To print
Hyper-V Quick Create
09:32
27/06/2018
TOM CLANCY'S
GHOST RECON
WILDLANDS


Untitled - Notepad
File Edit Format View Help
DemoDB.kdbx - KeePass
File Edit View Tools Help
Search...
DemoDB
General
Windows
Network
Internet
Recycle Bin
Title
User Name
Password
URL
Notes
All the switches
USERNAME
0 of 1 selected
Ready.
TOM CLANCY'S
GHOST RECON
WILDLANDS


UNIFY
79145
GHOST RECON
F-35



YubiKey

Register your YubiKey

Go to the Security Settings of a supported service, select two-factor authentication using a security key, and follow setup instructions.

Insert YubiKey & tap

Insert the YubiKey into a USB-port and touch the golden area of the security key, verifying that you are not a remote hacker.

Tap on phone

For NFC-enabled Android phones, just tap a YubiKey NEO against the phone to complete authentication.

		
YubiKey 4	YubiKey Neo	Security Key by Yubico
‘The one we use’	‘The one we would use if we needed NFC’	‘The one that you would get your security minded brother/sister for a birthday present’*
Great smart card support FIDO U2F Key printer, OpenPGP, OATH-TOTP, OATH-HOTP, and Challenge-Response	Nearly great smart card support FIDO U2F Key printer, OpenPGP, OATH-TOTP, OATH-HOTP, and Challenge-Response NFC (works with Paxton Net2 and Salto)	FIDO U2F FIDO2
£36.50 on Amazon.co.uk	£45.50 on Amazon.co.uk	£18 on Amazon.co.uk

Prices on 27/06/2018


fido U2F
YubiKey 4C Nano
YubiKey 4C
YubiKey 4 Nano
YubiKey 4

Smart Cards

UNIVERSITY OF OXFORD

Christopher M Wren

UNDERGRADUATE reading for
MMathPhil Mathematics & Philosophy

Mathematical Institute

136

12345

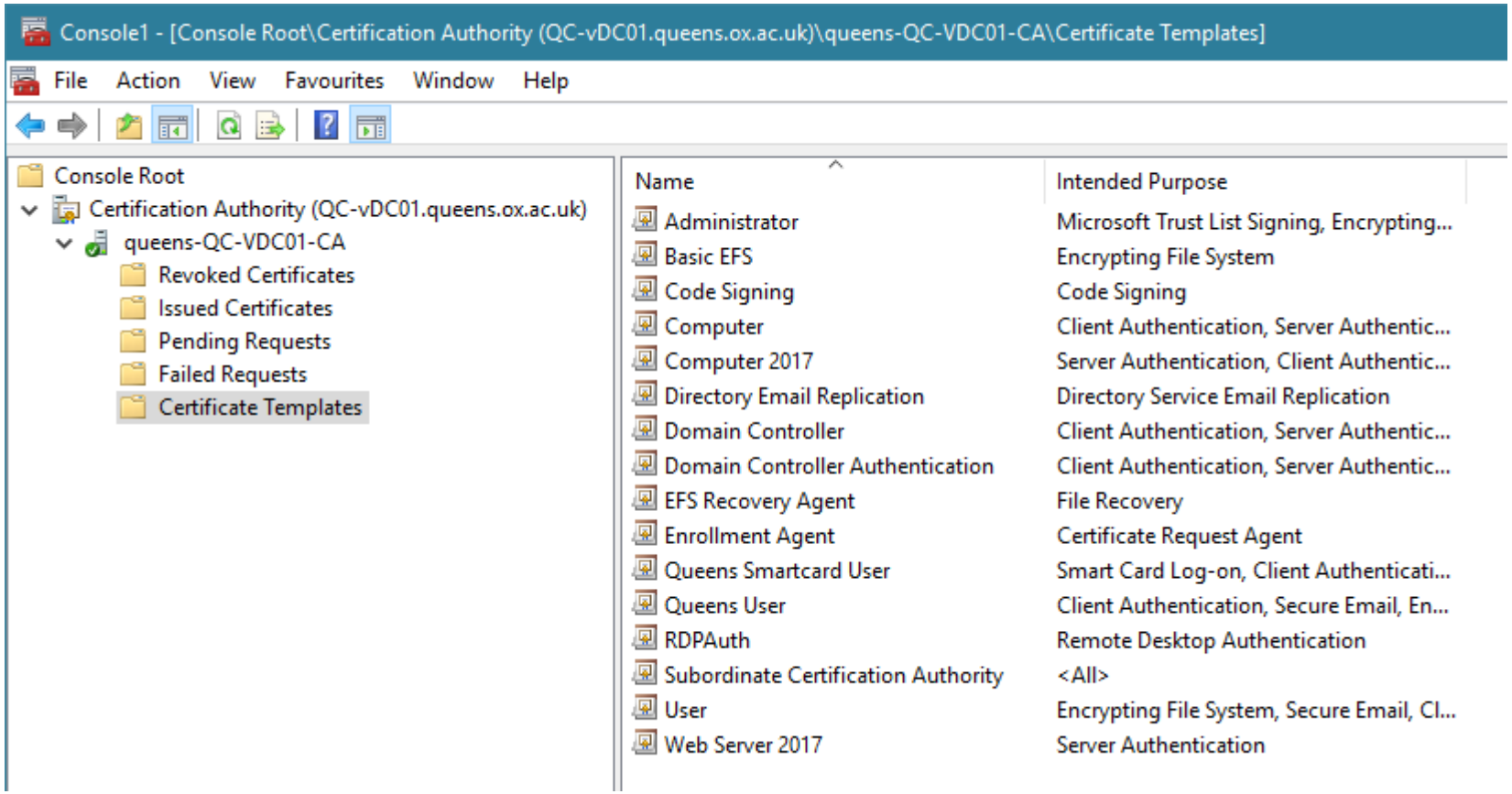
VALID UNTIL
30 JUN 2017

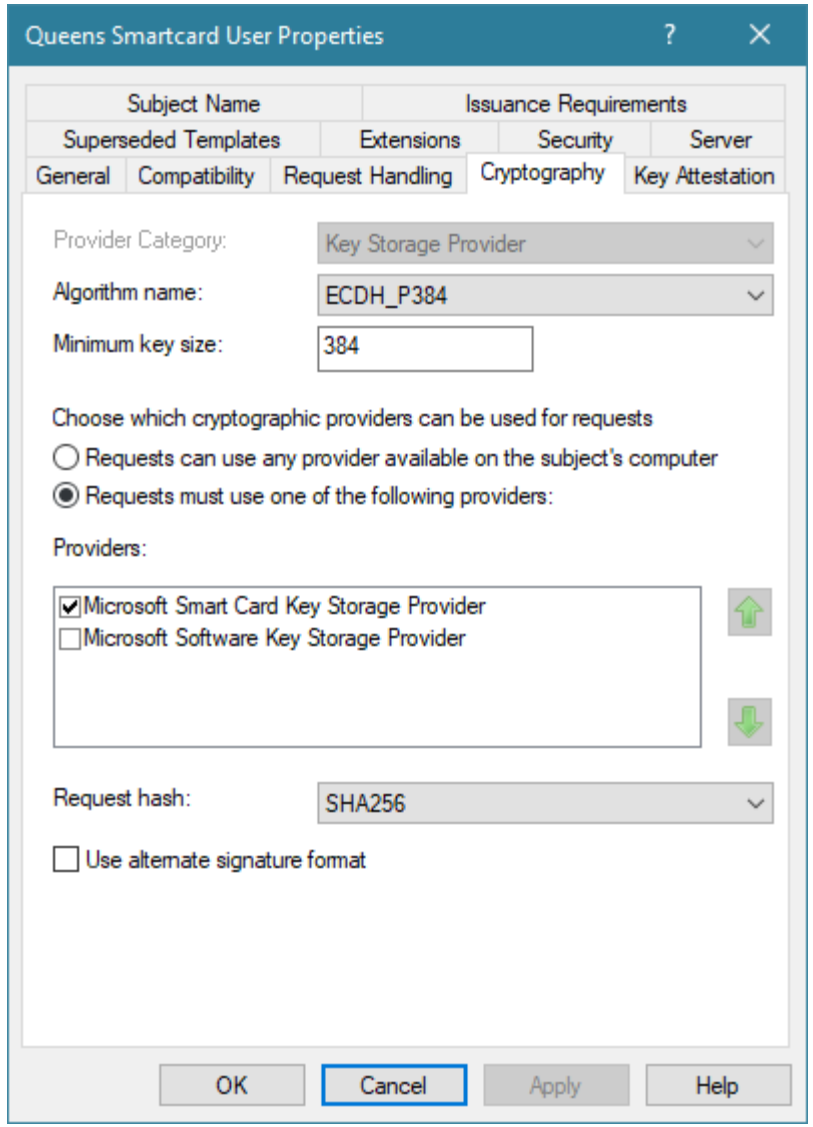
S 2804772


HID
Mitzi Jones
Emp.# 5643-44
HID
OMNIKEY


HID
Crescendo® C1150
Smart Card


gemalto
Microso


Console1 - [Console Root\Certification Authority (QC-vDC01.queens.ox.ac.uk)\queens-QC-VDC01-CA\Certificate Templates]
File Action View Favourites Window Help
Console Root
Certification Authority (QC-vDC01.queens.ox.ac.uk)
queens-QC-VDC01-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
Administrator
Microsoft Trust List Signing, Encrypting...
Basic EFS
Encrypting File System
Code Signing
Code Signing
Computer
Client Authentication, Server Authentic...
Computer 2017
Server Authentication, Client Authentic...
Directory Email Replication
Directory Service Email Replication
Domain Controller
Client Authentication, Server Authentic...
Domain Controller Authentication
Client Authentication, Server Authentic...
EFS Recovery Agent
File Recovery
Enrollment Agent
Certificate Request Agent
Queens Smartcard User
Smart Card Log-on, Client Authenticati...
Queens User
Client Authentication, Secure Email, En...
RDPAuth
Remote Desktop Authentication
Subordinate Certification Authority
<All>
User
Encrypting File System, Secure Email, Cl...
Web Server 2017
Server Authentication


Queens Smartcard User Properties
Subject Name
Issuance Requirements
Superseded Templates
Extensions
Security
Server
General
Compatibility
Request Handling
Cryptography
Key Attestation
Provider Category:
Key Storage Provider
Algorithm name:
ECDH_P384
Minimum key size:
384
Choose which cryptographic providers can be used for requests
Requests can use any provider available on the subject's computer
Requests must use one of the following providers:
Providers:
Microsoft Smart Card Key Storage Provider
Microsoft Software Key Storage Provider
Request hash:
SHA256
Use alternate signature format
OK
Cancel
Apply
Help

YubiKey Smart Card Deployment Guide

Best Practices and Basic Setup

YubiKey 4 Series (YubiKey 4, YubiKey 4 Nano, YubiKey 4C, YubiKey 4C Nano)
YubiKey NEO Series (YubiKey NEO, YubiKey NEO-n)

Last Updated: 3/2/2018

yubico

The following topics are covered in this document:

Getting Additional Help

For more information, and to get help with your YubiKeys, see:

- Support home page
- Documentation and FAQs
- Start a Support ticket

TIP: To assist in diagnosing issues, we recommend that you include a log file containing the issue observed. To enable the debug log file, add the following registry key. Log files will be created for each running process in C:\Logs.

Key: HKLM\Software\Yubico\ykmd
Value: DebugOn (DWORD) - to enable logging set value to 1.

- If you need assistance with Microsoft tools or products, contact Microsoft directly.

yubico

Creating a Certification Authority

If a Certification Authority already exists in your environment, skip this section and proceed to YubiKey Minidriver Installation.

Creating a Certification Authority:

1. Open Server Manager and choose **Add roles and features**, and click **Next**.
2. Select **Role-based or feature-based installation**, and click **Next**.
3. Select **Select a server from the server pool**.
4. From **Server Pool**, select the server on which you want to install the Certification Authority, and click **Next**.
5. Under **Server Roles**, select **Active Directory Certificate Services**, and click **Next**.
6. Click **Add Features**, and click **Next**.
7. Click **Next** again.
8. Select **Certification Authority**, and click **Next**.
9. Click **Install**. Allow several minutes for the process to complete.
10. Select **Configure Active Directory Certificate Services on the destination server**, and click **Next**.
11. Select **Certification Authority**, and click **Next**.
12. Choose **Enterprise CA**, and click **Next**.
13. Choose **Root CA**, and click **Next**.
14. Select **Create a new private key**, and click **Next**.
15. Select the **cryptographic provider**, **hash algorithm**, and **key length** for the private key, and click **Next**.
    NOTE: Changing the **cryptographic provider**, **hash algorithm**, and **key length** from the default values may increase the size of smart card login certificates beyond the available space on the YubiKey. Be sure the values you select are supported by the YubiKeys that you will use in your environment:

	Maximum supported certificate size	Supported key lengths (bits)	Supported hash algorithms	Encryption
YubiKey NEO	2048 bytes	RSA: 1024, 2048	SHA1, SHA256	RSA
YubiKey 4	3072 bytes	RSA: 1024, 2048 ECDSA: P256, P384	SHA1, SHA256, SHA384	RSA; ECDH

16. **Common name** and **Distinguished name** will be automatically populated. Confirm the values match the server name and domain name, and click **Next**.
17. Select the **validity period** for the Certification Authority certificate, and click **Next**.
    TIP: This period must be longer than what you set for the smart card login certificate template. Yubico recommends the default value of **5 years**.
18. Leave the Database locations to the default values and click **Next** again.
19. Verify all settings match the desired values, and click **Configure**.
20. When the process completes, exit the installation wizard by clicking **Close**.

yubico

Setting the PIN

Once a YubiKey is registered, the user's PIN should be changed if the default value (123456) is still set. Once the user has logged into his account, he can change the PIN of a YubiKey connected to his system as follows:

1. Use **Ctrl+Alt+Del** to enter the lock screen.
2. Select **Change a Password** from the options presented.
3. The user is prompted to enter the current PIN, as well as the new PIN.
4. Press Enter to commit the new PIN.

PIN Unblock

By default, the user PIN is blocked when three consecutive incorrect PINs have been entered. The PIN Unblock Code (PUK) is used for unblocking the User PIN. If both the PIN and the PUK are blocked, the YubiKey must be reset, which deletes any loaded certificates and returns the YubiKey to a factory default state.

The YubiKey Minidriver will block the PUK if it is set to the factory default value. Once the PUK is blocked, it cannot be used unless the PIV applet is reset. To use the PUK, it must be first set with the Yubico PIV Tool before using the YubiKey Minidriver to load or modify certificates on the YubiKey PIV Applet.

If using the YubiKey PIV tool, the command below will prompt the user to set a new PUK value:

```
yubico-piv-tool -achange-puk
```

The current and new values for the PUK should be entered in alphanumeric text. These values are not automatically recorded, and should be noted for future use.

When unblocking the PIN via the Windows 7, Windows Server 2008, and Windows Server 2008 R2 logon interface, Windows requires the PIN unblock code (PUK) to be typed in as hexadecimal digits. This means that if your PUK is "12345678, to unblock a pin through the Windows UI, you must type the ASCII hex-encoded bytes of the PUK string (in this case, the unblock code would be 3132333435363738). Refer to an ASCII chart (for example, www.asciitable.com) to encode a PUK in hexadecimal.

To unblock the user PIN:

1. With the YubiKey inserted, attempt to log in at the Windows login screen. When the PIN is blocked, the "change a password" screen is displayed. The following screenshot is an example using Windows 10.

2. Select the checkbox for **Unblock smart card**.
3. On Windows 7 and Windows Server 2008 R2 SP1 enter the in the Response field in hexadecimal format, (example: the default value of 12345678 in hexadecimal format is

yubico

Generating and importing user certificates as a .pfx file

In environments where the user certificates cannot be generated on the YubiKey, they can be generated on a Windows PC as a .pfx file and imported to a YubiKey for use.

To use an enrollment agent to generate a .pfx file for import:

1. Right-click the Windows Start button and select **Run**.
2. Type `mmc` and press Enter.
3. Add a Certificates snap-in for My User account.
4. In the console tree, expand the Personal store, and then click Certificates.
5. On the Action menu, point to All Tasks, point to Advanced Operations, and then click Enroll on behalf of to open the Certificate Enrollment wizard. Click Next.
6. Browse to the Enrollment Agent certificate that you will use to sign the certificate request that you are processing. Click Next.
7. Select the type of certificate that you want to enroll for. When you are ready to request a certificate, click Enroll.
8. After the Certificate Renewal Wizard has successfully finished, click Close.

Exporting a certificate with Private Key

1. On the workstation where you enrolled the smart card certificates, choose **Start**, choose **Run**, and then in the Open box, type `mmc`. Choose **OK**.
2. On the Console page, on the File menu, select Add/Remove Snap in.
3. On the Add/Remove Snap-in dialog box, choose **Add**. The Add Standalone Snap-in page appears. Select **Certificates** and then choose **Add**.
4. On the Certificates snap-in page, select **My user account**, and then choose **Finish**. On the Add or Remove Snap-in page, choose Close, and then on the Add/Remove Snap-in page, choose OK.
5. On the Console page, in the navigation pane, expand **Certificates - Current User** – and then expand **Personal**. In the navigation pane, select **Certificates**.
6. In the details pane, locate the certification authority certificate that was issued for the Smart Card Logon. Right-click the Smart Card Logon certificate for your Smart card user. **Right-click** this Certificate, select **All Tasks**, and then choose **Export**.
7. The Welcome to the Certificate Wizard dialog box appears. Choose **Next** to continue.
8. On the Export Private Key page, select **Yes**, export the private key. Choose **Next**.
9. On the Export File Format page, make sure that you select Personal Information Exchange – PKCS #12 (.PFX). Make sure that you select the Enable strong protection box. Choose **Next**.
10. On the Password page, supply a password, and then choose **Next**.
11. On the File to Export page, type the path and filename of the .pfx file. For example, C:\usercert.pfx. Choose **Next**.
12. Choose Finish. On the Certificate Export Wizard page, choose **OK** to confirm that the export was successful.
13. Repeat steps 7 through 12. For each user certificate to export.

Importing a .pfx file using Certutil

1. On the workstation where you enrolled the smart card certificates, choose **Start**, choose **Run**, and then in the Open box, type `CMD`. Choose **OK**.
2. On the Command Line Interface, enter the command:
   `certutil -f -user -p "Microsoft Base Smart Card Crypto Provider" -importpfx certname.pfx`
   Where certname.pfx is the name of the .pfx file to import.
3. Repeat step 2 for each .pfx file to import.

yubico

Basic Troubleshooting

- If I YubiKey is connected to a computer when installing the YubiKey Minidriver, Windows may continue to use the native generic smart card minidriver. The YubiKey Minidriver can be set as the default driver by following these steps:
  - Connect your YubiKey to your computer
  - Open up **Device Manager**
  - Locate the YubiKey smart card entry - it will be labeled **Identity Device (NIST SP 800-73 [PIV])**. Right click the entry and select **Update driver**.
  - In the window which opens, select **Search automatically for updated driver software**
  - A list of drivers will be displayed. Select **YubiKey Minidriver**.
- The YubiKey NEO, when trying to enroll a certificate larger than the supported maximum key size of 2048 bits may freeze unexpectedly. For larger certificates, it is recommended to use the YubiKey 4 hardware.
- When attempting to import a certificate into the YubiKey 4 when the card has reached its maximum storage of 12 certificates, the certutil program may show an inconsistent number of certificates.
  Use the following command to list the keys seen by the YubiKey Minidriver along with their associated container names:

  ```
  certutil -key -csp "Microsoft Base Smart Card Crypto Provider*
  ```

  Use the following command to delete a specific key:

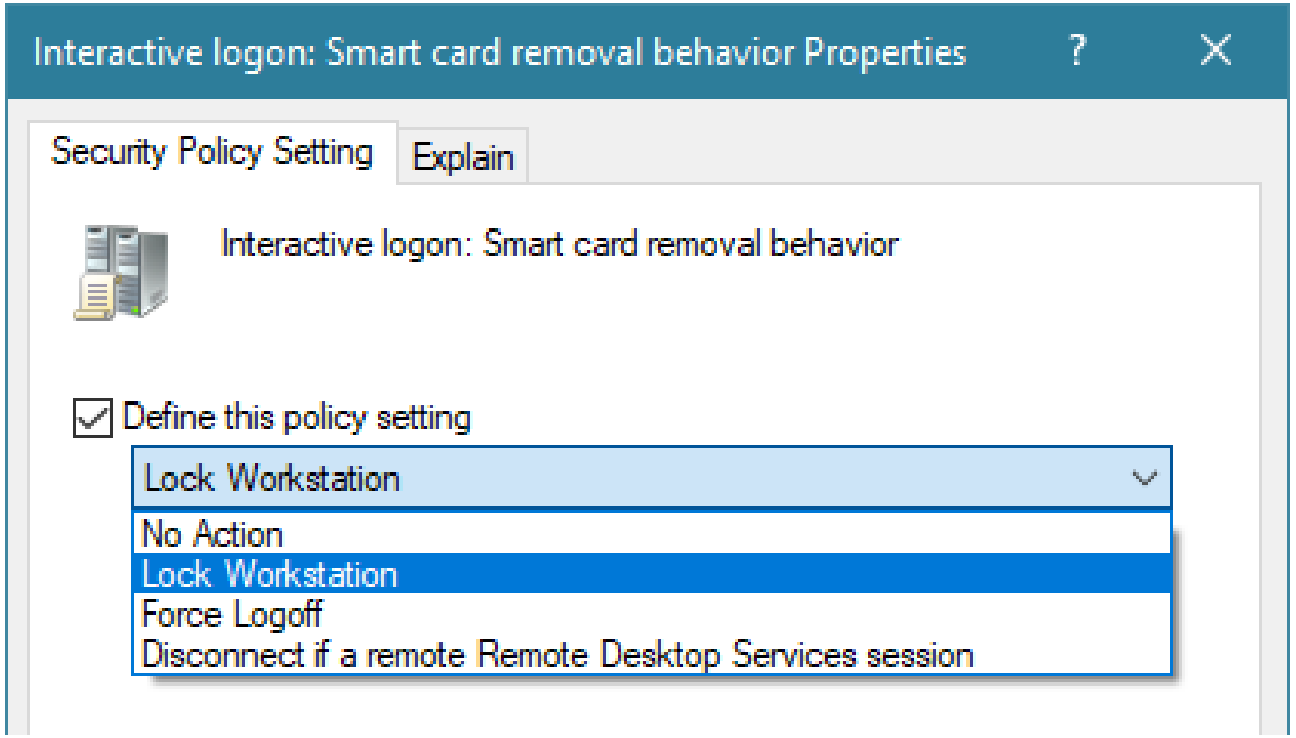
  ```
  certutil -delkey -csp "Microsoft Base Smart Card Crypto Provider*" "<container name>"
  ```

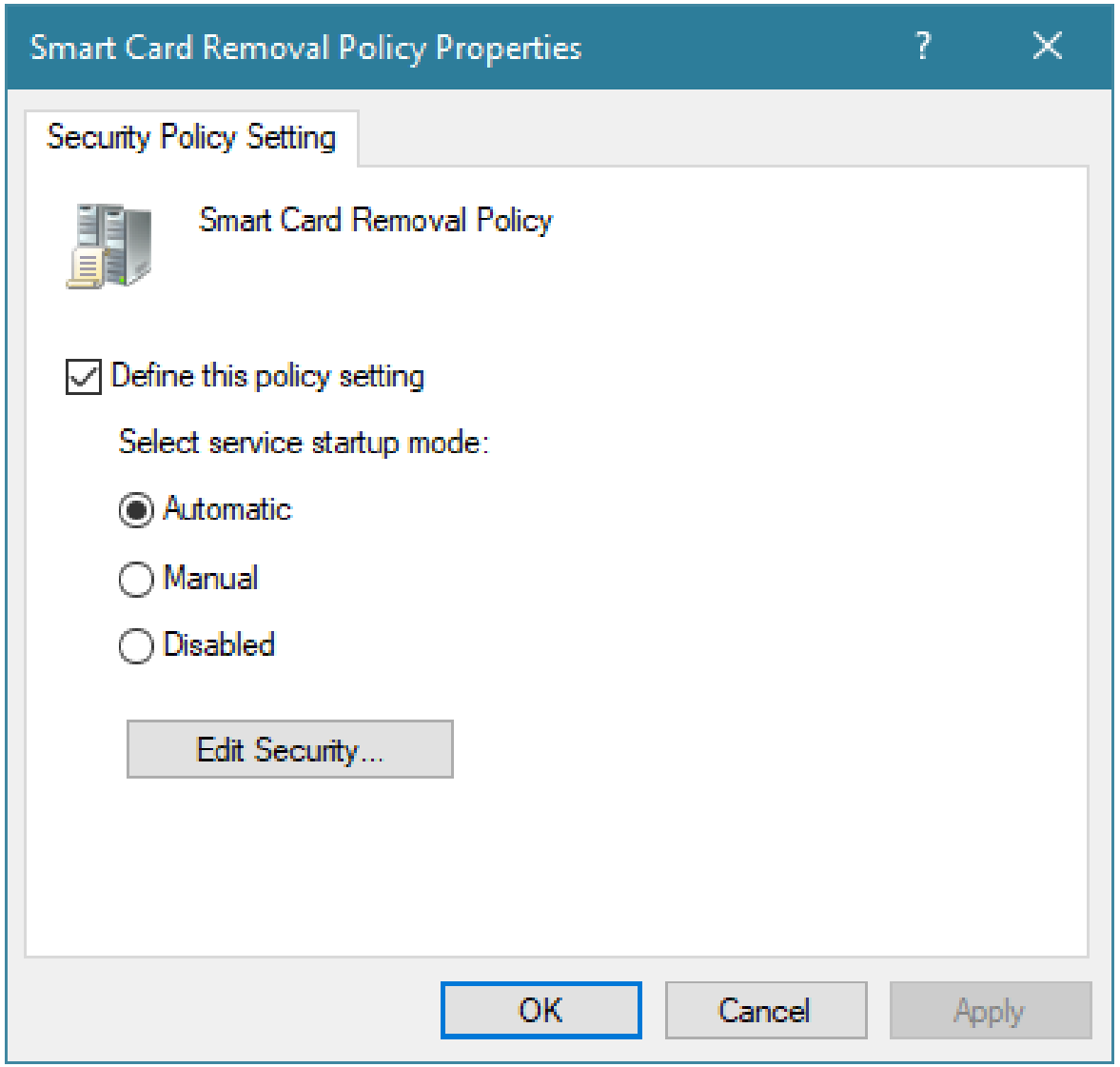
- Due to a limitation with the legacy CSP, the Microsoft Base Smart Card Crypto Provider will not see any ECC certificates or keys. To view ECC certificate and key information, use the Smart Card Key Storage Provider:

  ```
  certutil -csp "Microsoft Smart Card Key Storage Provider"
  ```

  We recommend you use the "Microsoft Smart Card Key Storage Provider" for better security and functionality.

- The Microsoft Smart Card Key Storage Provider does not support importing ECC keys and certificates through the certutil program. This is a limitation of the certutil program.
- Windows 7 may not be able to verify code integrity of the YubiKey Minidriver DLL (ykmd.dll) due to the BHA256 signature of Yubico's code signing certificate. If you see a "Bad Image" warning when running certutil or see error 3002 in the Microsoft Windows CodeIntegrity Operational log, apply update KB3033929 to resolve this issue.


Interactive logon: Smart card removal behavior Properties
Security Policy Setting
Explain
Interactive logon: Smart card removal behavior
Define this policy setting
Lock Workstation
No Action
Lock Workstation
Force Logoff
Disconnect if a remote Remote Desktop Services session


Smart Card Removal Policy Properties
Security Policy Setting
Smart Card Removal Policy
Define this policy setting
Select service startup mode:
Automatic
Manual
Disabled
Edit Security...
OK
Cancel
Apply

Setting Touch Policy

The YubiKey can be set to require a physical touch to confirm any cryptographic operations. This is an optional feature to increase security, ensuring that any authentication operation must be carried out in person. The YubiKey Minidriver sets the touch policy are set when a key is first imported or generated. Once set for a key on the YubiKey, the policies cannot be changed.

By default, the touch policy for keys imported/generated through the minidriver is created with the default setting of the touch policy disabled.

To alter the policy behavior, the registry must be configured prior to setting up keys, either on the station enrolling the keys or pushed out to all machines using Group Policy Objects.

Key: **HKLM\Software\Yubico\ykmd**

Value: **NewKeyTouchPolicy** (DWORD) - sets the touch policy on new keys generated/imported through the minidriver. Accepted values are:

- **1 <Never>** - Default policy of never requiring a user touch
- **2 <Always>** - Policy is set to require a user touch to confirm each and every cryptographic operation. Yubico does not recommend using this setting, as some Windows services, such as login, may require multiple cryptographic operations in a short time span.
- **3 <Cached>** - Policy is set to require physical touch once, then allow for cryptographic operations in a small time window afterwards. For using the physical touch option with Windows Smart Card Logon, this option is required.

Smart Cards – What we really like

- Unplug your card – auto PC lock
- Multiple credentials – one PIN (or many with the right kit)
- Login to web applications (that support certificates)
- Can be used with Get-Credential in PowerShell ;)

KeePass

Features

- Free – open source
- Loads of encryption jargon that sounds good
- Import/Export to a variety of formats
- Double click to clipboard and auto type
- Built in password generator
- So so so many plugins
- Data all stored in a single file
- Nothing in ‘the cloud’

Backup & Synchronization & IO

Another Backup Plugin
Automatically backs up databases.
DB_Backup
Creates backups of databases.
DataBaseBackup
Creates backups of databases.
SimpleDatabaseBackup
Creates backups of databases.
IOProtocolExt
Adds support for SCP, SFTP and FTPS.
SftpSync
Adds support for SFTP.
KeeAnywhere
Adds support for online storage providers.
KeeCloud
Adds support for online storage providers.
KeePassSync
Synchronize using online storage providers.
KPDataSave (Dropbox)
Save your database in Dropbox.
KPGoogleSync
Synchronize using Google Drive.
KeePassOneDriveSync
Synchronize using OneDrive.
CyberGate Password Vault Plugin
Adds support for communicating with CyberGate Password Vault.

Utilities

AdvancedConnect
Allows to specify applications for direct connections.
AutoTypeCustomFieldPicker
Allows to pick a custom field during auto-type.
AutoTypeSearch
Provides quick searching as enhancement to global auto-type.
AutoTypeShow
Shows an entry after auto-typing.
~~**ChkForUpd**~~
~~Checks periodically for new KeePass releases.~~
CheckPasswordBox
Prevents auto-typing passwords into wrong places.
Custom Icon Dashboarder
Statistics and management features for custom icons.
~~**DataBaseReorder**~~
~~Reorders groups alphabetically.~~
HaveIBeenPwned
Checks entries against breach lists.
HIBPOfflineCheck
Checks passwords against a breach list.
iTanMaster
Advanced indexed security token management.
KeeAutoExec
Automatically opens additional databases.
KeePassHIBP
Checks passwords against a breach list.
KeePassTimestampChanger
Allows to change timestamps.
KPEntryTemplates
Allows to design new entry types based on templates.
KPEnhancedListView
Extends the KeePass entry list.
KPEnhancedEntryView
Extends the KeePass entry view.
KPFieldsAdminConsole
Get statistics and perform bulk operations on fields.
LockExtensions
Provides more ways to lock the database.
MinLock
Keeps a minimized KeePass locked.
On-Screen Keyboard
Extends KeePass by an on-screen keyboard functionality.
On-Screen Keyboard 2
Extends KeePass by an on-screen keyboard functionality.
Password Counter
Counts and shows entries sharing a password.
Passphrase Generators
Generate passphrases.
PEDCalc
Allows to define a default lifetime for passwords.
Pronounceable Password Generator
Generates pronounceable passwords.
QualityColumn
Provides a 'Password Quality' column.
QualityHighlighter
Highlights entries based on the password quality.
QuickConnectPlugin
Connects to Windows/Linux/ESXi hosts.
QuickSearch
Provides enhanced search capabilities.
RDPPlugin
Connects to a server via RDP.
KeeResize
Makes dialogs resizable.
RmvDup
Removes duplicate entries and empty groups.
StrengthReport
Creates password strength reports.
TAN Placeholder
Adds support for a placeholder that retrieves a TAN.
Title Display
Customize main window title display.
TrayRecentFiles
Lists recent files in the system tray icon menu.
TrueCrypt/VeraCrypt Mount
Mounts TrueCrypt/VeraCrypt volumes.
TrueCrypt/VeraCrypt AutoDismount
Automatically dismounts TrueCrypt/VeraCrypt volumes.

Integration & Transfer

KeeForm
Opens websites and fills in the login data automatically.
Kee
Bridge between KeePass and web browsers.
PassIFox
Replaces the built-in Firefox password storage by KeePass.
ChromeIPass
Integrates KeePass and the Google Chrome browser.
Passafari
Integrates KeePass and the Safari browser.
URL in Title Bar
Browser extensions that show the current URL in the title bar (for multiple browsers).
KeePasser
Allows auto-typing into webforms based on URLs (Internet Explorer and Maxthon).
KPFloatingPanel
Displays an always on top KeePass floating panel.
KeePassHelper
Browser extension that retrieves credentials from KeePass.
WebAutoType
Allows auto-typing into webforms based on URLs (multiple browsers).
RDCAutoTypeAndTCATO
RDC auto-type support and improved TCATO selection.
TCATO Placeholder
Allows to enable/disable TCATO per auto-type sequence.
HotKeyEnabler
Allows to define custom sequences of keys system-wide with auto-type functionality.
KeeOtp
Generates TOTP authentication codes.
Tray TOTP
Generates TOTP authentication codes.
Character Copy
Allows copying individual characters from entry strings.
QrCodeGenerator
Displays passwords as QR codes.
KeePassQRCodeView
Displays entry fields as QR codes.
KeePT
Integrates GPG/WinPT functionality.
PuttyAgent
Adds SSH agent support to KeePass.
KeeAgent
Adds SSH agent support to KeePass.
Remote Desktop Manager Plugin
Allows KeePass to supply credentials to Remote Desktop Manager.
KeePassRest
Allows KeePass to supply credentials e.g. to SmartFTP.
KeePassRPC
Allows KeePass to supply credentials via RPC.
KeePassHttp
Allows KeePass to supply credentials via HTTP.
KeeSAPLogon
Logon to SAP systems.
SalesforcePlugin
Logon to Salesforce environments.
Ubuntu Integration Plugins
Plugins to help KeePass integrate better with the Ubuntu desktop.

Cryptography & Key Providers

CertKeyProvider
Advanced certificate-based key provider.
Multi Cert Key Provider
RSA certificate-based key provider.
RSA Cert Key Provider
Simple RSA certificate-based key provider.
KeyManager
Certificate-based key provider with GUI.
Smart Certificate Key Provider
Certificate-based key provider with smart card support.
OtpKeyProv
Key provider based on one-time passwords.
KeeChallenge
Key provider based on challenge-response.
Key Xchanger
A bluetooth key provider plugin.
WinKee
Manages database access credentials.
KeePassQuickUnlock
Allows you to unlock databases quickly.
KeePassRFID
Key provider using RFID/NFC smart cards.
LoginCard Key Provider
Key provider using RFID LoginCard (OWOK light).
KeePassKeyServer
Key provider that retrieves a key from a key server.
Twofish Cipher
Adds the Twofish encryption algorithm.
Serpent Cipher
Adds the Serpent encryption algorithm.
Salsa Cipher
Adds the Salsa20 encryption algorithm.
GostPlugin
Adds the GOST R 34.12-2015 encryption algorithm.
MultiCipher
Dual encrypts databases using AES-256 and 3DES-192.

Import

1P2KeePass
Imports 1Password 1PIF files.
AnyPassword Import
Imports CSV files exported by 'AnyPassword'.
CardFileKPPlugin
Imports CRD files created by 'Cardfile'.
CodeWallet 3 Import
Imports TXT files exported by 'CodeWallet 3'.
CodeWallet 6 Konverter
Converts TXT files exported by 'CodeWallet 6' to importable CSV files.
eWallet Import
Imports TXT files exported by 'eWallet'.
eWallet Data Liberator
Export data from 'eWallet' and import it into KeePass.
eWallet to KeePass
Migrate 'eWallet' data to KeePass.
Firefox to KeePass Password Importer
Imports passwords from Firefox into KeePass.
KeePassBrowserImporter
Imports credentials from various browsers.
MSDN/TechNet Key Importer
Imports MSDN/TechNet key files.
Oubliette Import
Imports Oubliette password database files.
PasscommImport
Imports Password Commander CSV files.
Password Minder Import
Imports Password Minder data.
PINs Import
Imports text files exported by 'PINs'.
PwSafeDBImport
Directly import Password Safe database files.
SafeInCloudImp
Imports SafeInCloud XML files.
SpmImport
Imports Steganos Password Manager files.
VariousImport
Imports several different file formats.
Vault3Importer
Imports Vault3 XML files.
VaultSyncPlugin
Imports HashiCorp Vault data.
XML Import
Imports XML files exported by KeePass 1.x.
ZSafe Import
Imports text files exported by 'ZSafe'.
Convert to 1.x CSV
Utilities to convert text files to KeePass 1.x CSV files.
Convert to 1.x XML
Utilities to convert text files to KeePass 1.x XML files.
Convert to 2.x XML
Utilities to convert text files to KeePass 2.x XML files.
Favicon Downloader
Download and store website favicons.
Yet Another Favicon Downloader
Download and store website favicons.

Export

KeePassNewKeyExport
Export data with a new master key.
Partial KeePass Database Export
Export tagged entries.
KeePassSubsetExport
Export tagged entries.
KeeOldFormatExport
Export to old KeePass file formats.
KdbxLite
Creates lite KDBX files.
SecExchange
Send entries via Secure Exchanges.
Seclave Plugin
Export to Seclave password manager device.
TheVaultExport
Export to The Vault CSV files.
KeePass to Keyring
Export KeePass data to Keyring files.
KeePassIPhone
Convert KeePass 1.x files to iPhone bookmarklets.

Import & Export

KeeToReady
Imports/exports records from/to ReadySignOn.
MSWifiPlugin
Exchange wireless connection information.

Automation & Scripting

KPScript
KeePass scripting utility.

Resources

Application Icons
Additional application icons.
Client Icons
Additional client icons.

For Developers Only

Sample Plugins
Show developers how plugins can perform basic operations.

Icons: = the plugin is available for KeePass 1.x, = the plugin is available for KeePass 2.x.

HaveIBeenPwned 2.x

Plugin Author: Andrew Schofield, Plugin Language:

This plugin checks entries against breach lists.

Passphrase Generators 2.x

The following plugins add password generator algorithms that create passphrases.

- **Readable Passphrase Generator**
  Extension Author: Murray Grant, Extension Language:

  The Readable Passphrase Generator plugin generates passphrases, which are (mostly) grammatically correct, but nonsensical. These are easy to remember (for humans), but difficult to guess (for humans and computers).

ChromeIPass 2.x

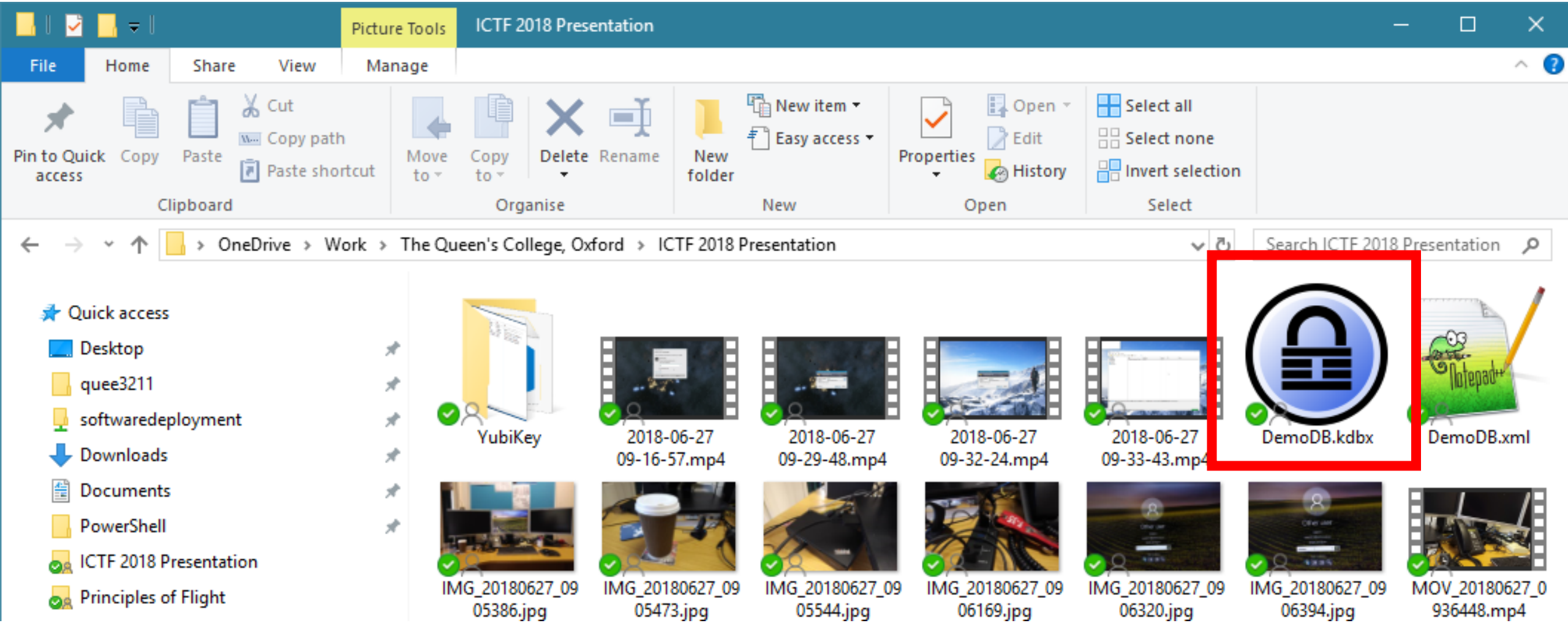
Extension Author: Perry Nguyen, Extension Language:

Extension allowing Google Chrome to form-fill passwords stored in KeePass.

Smart Certificate Key Provider 2.x

Plugin Author: BodnarSoft, Plugin Language:

Encrypt and decrypt your database using an X.509 certificate stored on a smart card or in the Windows Certificate Store.


Picture Tools
ICTF 2018 Presentation
File
Home
Share
View
Manage
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organise
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
OneDrive › Work › The Queen's College, Oxford › ICTF 2018 Presentation
Search ICTF 2018 Presentation
Quick access
Desktop
quee3211
softwaredeployment
Downloads
Documents
PowerShell
ICTF 2018 Presentation
Principles of Flight
YubiKey
2018-06-27 09-16-57.mp4
2018-06-27 09-29-48.mp4
2018-06-27 09-32-24.mp4
2018-06-27 09-33-43.mp4
DemoDB.kdbx
DemoDB.xml
IMG_20180627_095386.jpg
IMG_20180627_095473.jpg
IMG_20180627_095544.jpg
IMG_20180627_096169.jpg
IMG_20180627_096320.jpg
IMG_20180627_096394.jpg
MOV_20180627_0936448.mp4

KeePass
Password Safe

Home
- Home & News
- Forums
- Feature List
- Screenshots

Getting KeePass
- Downloads
- Translations
- Plugins / Ext.

Information / WWW
- Help
- FAQ
- Security
- Awards
- Links

Support KeePass
- Donate

Getting KeePass - Downloads

Here you can download KeePass:

KeePass 2.39.1

Installer for Windows (2.39.1):

Download Now
KeePass-2.39.1-Setup.exe

Download the EXE file above, run it and follow the steps of the installation program. You need local installation rights (use the Portable version on the right, if you don't have local installation rights).

Portable (2.39.1):

Download Now
KeePass-2.39.1.zip

Download the ZIP package above and unpack it to your favorite location (USB stick, ...). KeePass runs without any additional installation and won't store any settings outside the application directory.

Supported operating systems: Windows Vista / 7 / 8 / 10 (each 32-bit and 64-bit), Mono (Linux, Mac OS X, BSD, ...).

KeePass 1.35

Installer for Windows (1.35):

Download Now
KeePass-1.35-Setup.exe

Download the EXE file above, run it and follow the steps of the installation program. You need local installation rights (use the Portable version on the right, if you don't have local installation rights).

Portable (1.35):

Download Now
KeePass-1.35.zip

Download the ZIP package above and unpack it to your favorite location (USB stick, ...). KeePass runs without any additional installation and won't store any settings outside the application directory.

Supported operating systems: Windows Vista / 7 / 8 / 10 (each 32-bit and 64-bit), Wine.

Unsure which edition (1.x or 2.x) to choose? See the Edition Comparison Table. See also the Development Status FAQ. If in doubt, use KeePass 2.x.

https://keepass.info

KeeChallenge

A plugin for KeePass2 to add Yubikey challenge-response capability.

Download

View on GitHub

Supported Platforms

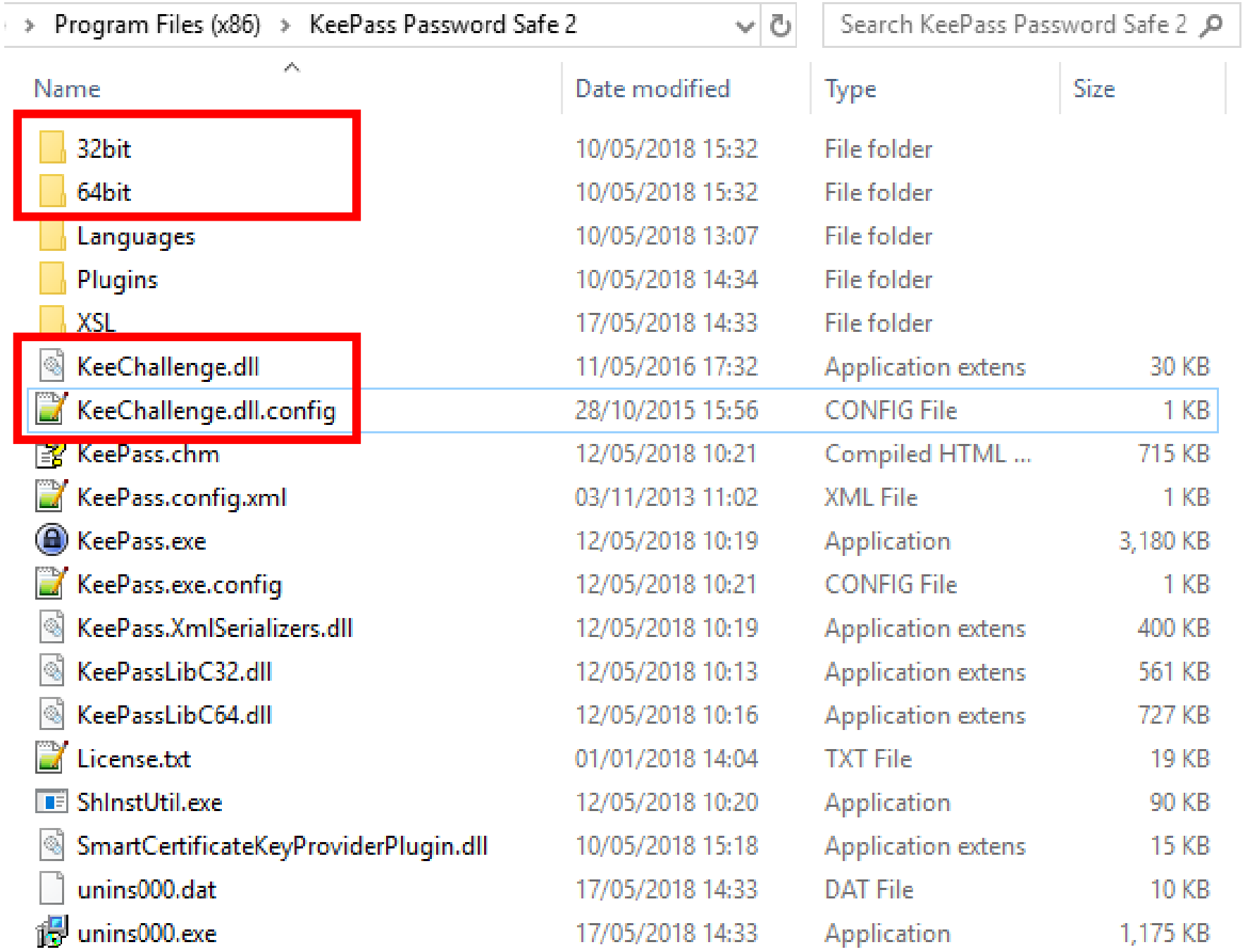
As of v1.0.1 both Windows and Linux (Ubuntu) have been tested successfully.

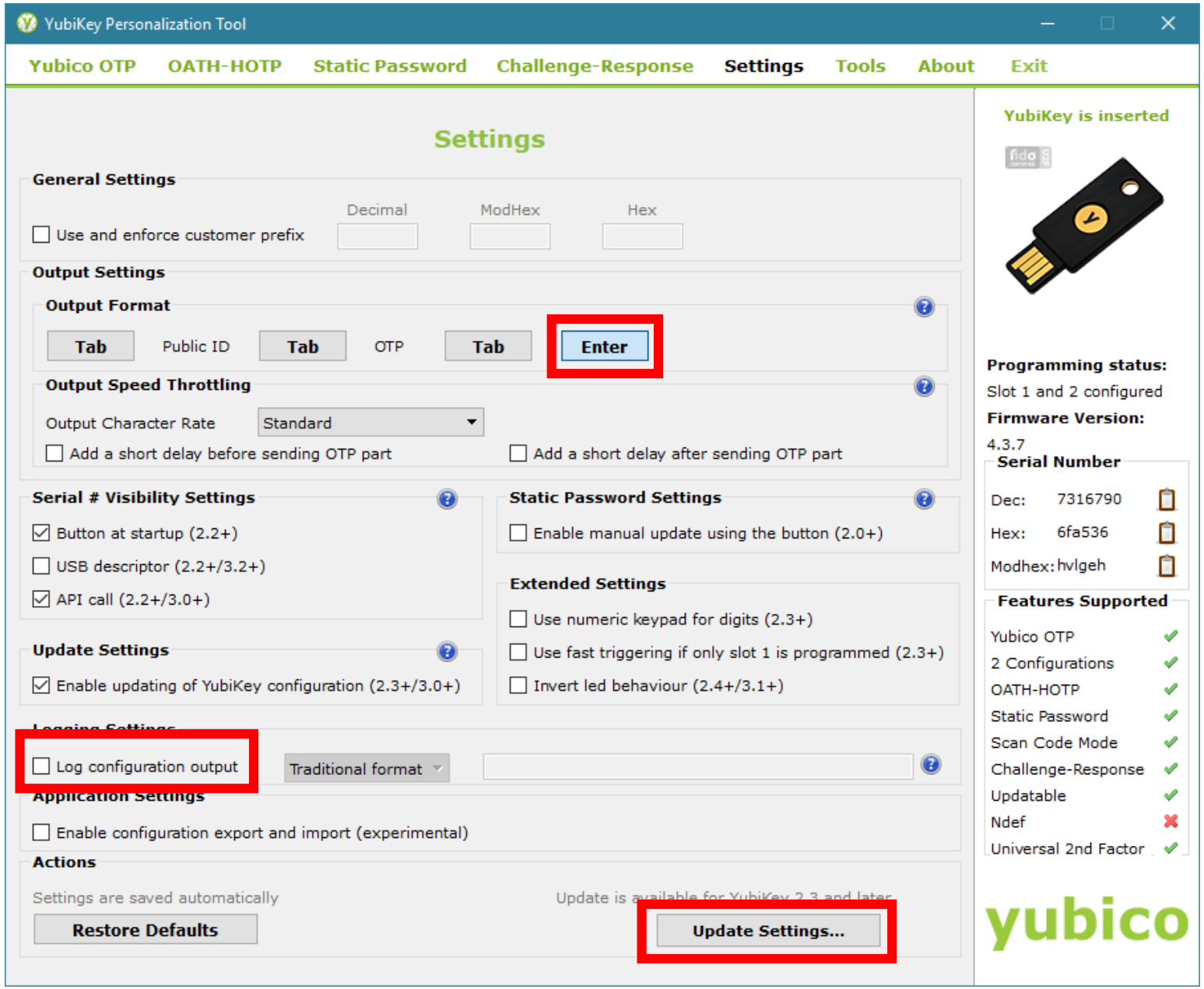
To run under Linux using mono, you must modify `KeeChallenge.dll.config` and add a dllmap entry to let Mono know where to find the native libraries. On my system this looks like `<dllmap dll="libykpers-1-1.dll" target="libykpers-1.so>`. For this to work, you must also obtain the appropriate versions of the Yubico libraries. Make sure all of the Yubico libraries are installed where mono can find them (for example, `/usr/lib`). Put both `KeeChallenge.dll` and `KeeChallenge.dll.config` in the KeePass2 folder (on Ubuntu this is `/usr/lib/keepass2`). The same technique will work on OSX, but getting the 32bit Yubico libraries requires building from source. See the OSX Guide by Markku for detailed instructions on how to do this.

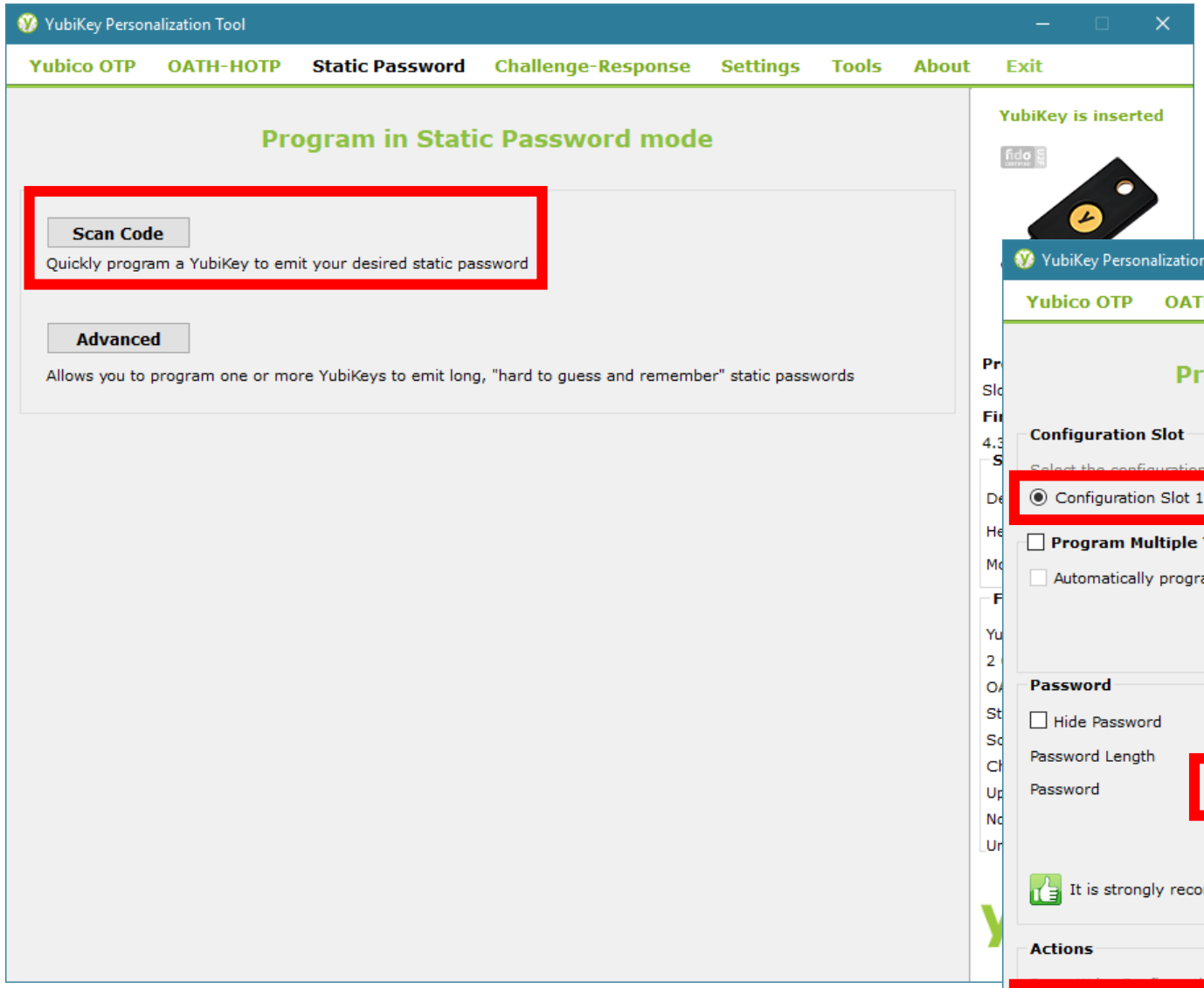
Dependencies

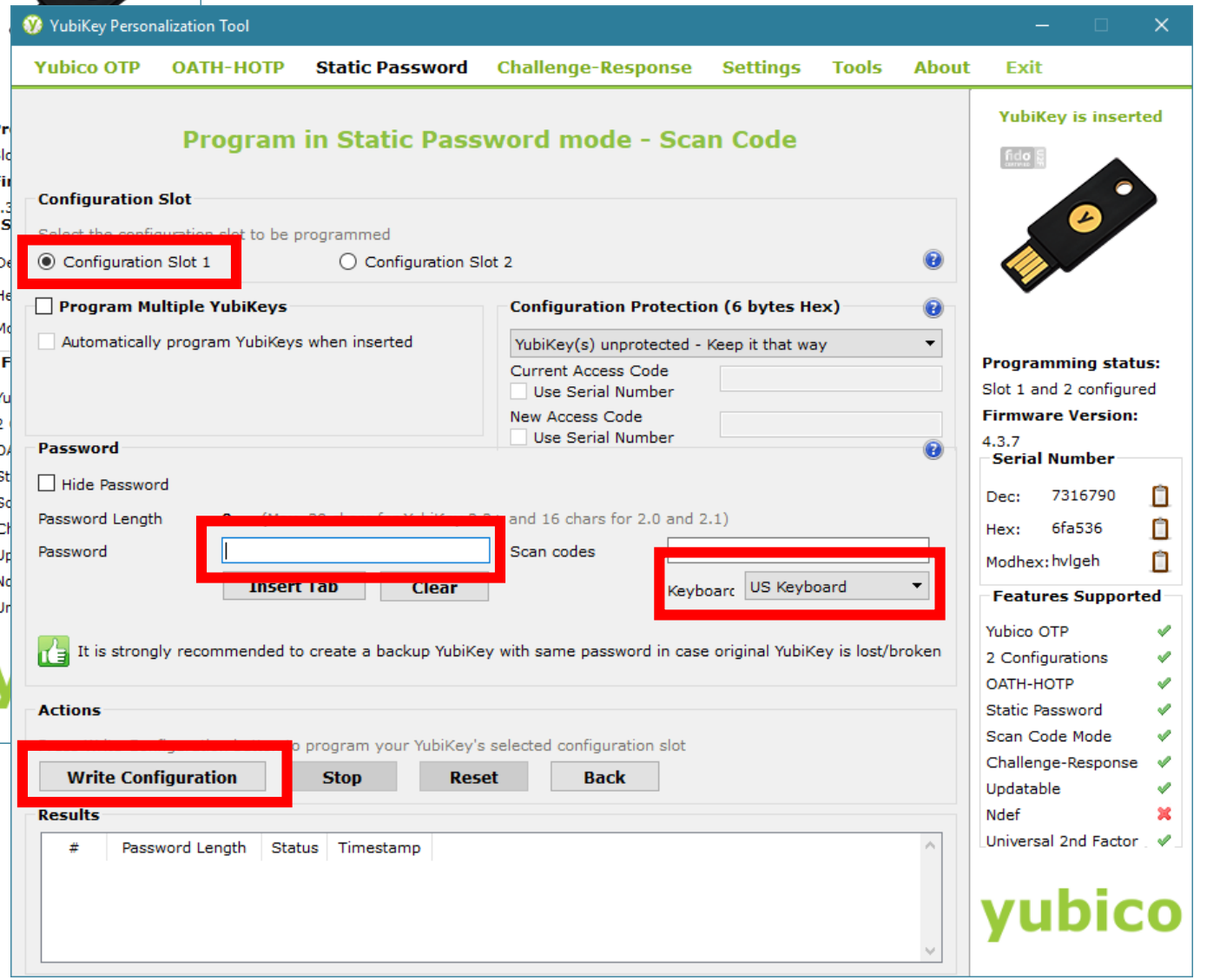
KeeChallenge requires KeePass2, available from http://keepass.info/download.html. It also requires the Yubico open source library yubico-personalization (which in turn depends on yubico-c). Prebuilt bundled binaries are available from http://opensource.yubico.com/yubikey-personalization/releases.html.

http://richardbenjaminrush.com/keechallenge

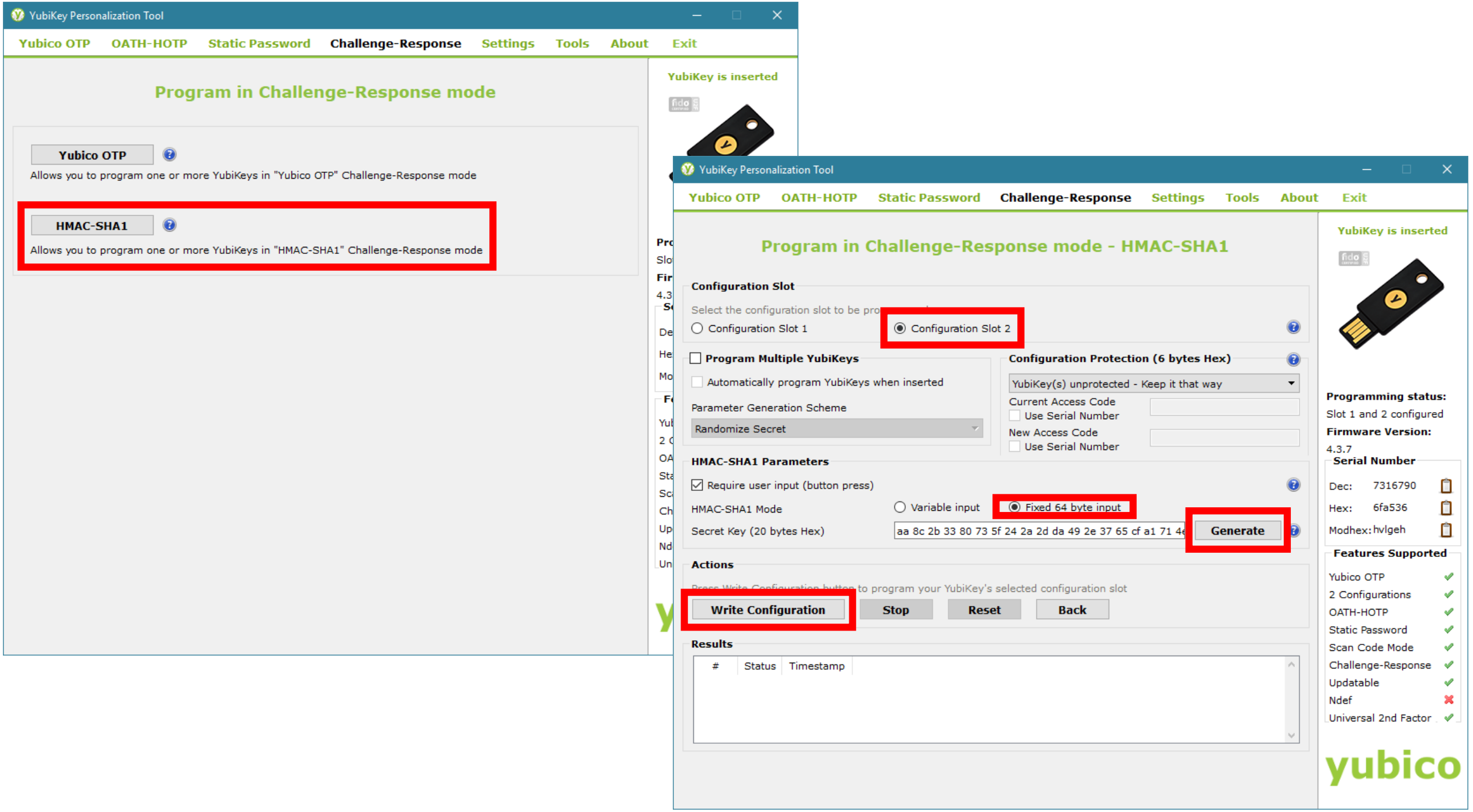

Program Files (x86) › KeePass Password Safe 2
Search KeePass Password Safe 2
Name
Date modified
Type
Size
32bit
10/05/2018 15:32
File folder
64bit
10/05/2018 15:32
File folder
Languages
10/05/2018 13:07
File folder
Plugins
10/05/2018 14:34
File folder
XSL
17/05/2018 14:33
File folder
KeeChallenge.dll
11/05/2016 17:32
Application extens
30 KB
KeeChallenge.dll.config
28/10/2015 15:56
CONFIG File
1 KB
KeePass.chm
12/05/2018 10:21
Compiled HTML ...
715 KB
KeePass.config.xml
03/11/2013 11:02
XML File
1 KB
KeePass.exe
12/05/2018 10:19
Application
3,180 KB
KeePass.exe.config
12/05/2018 10:21
CONFIG File
1 KB
KeePass.XmlSerializers.dll
12/05/2018 10:19
Application extens
400 KB
KeePassLibC32.dll
12/05/2018 10:13
Application extens
561 KB
KeePassLibC64.dll
12/05/2018 10:16
Application extens
727 KB
License.txt
01/01/2018 14:04
TXT File
19 KB
ShInstUtil.exe
12/05/2018 10:20
Application
90 KB
SmartCertificateKeyProviderPlugin.dll
10/05/2018 15:18
Application extens
15 KB
unins000.dat
17/05/2018 14:33
DAT File
10 KB
unins000.exe
17/05/2018 14:33
Application
1,175 KB

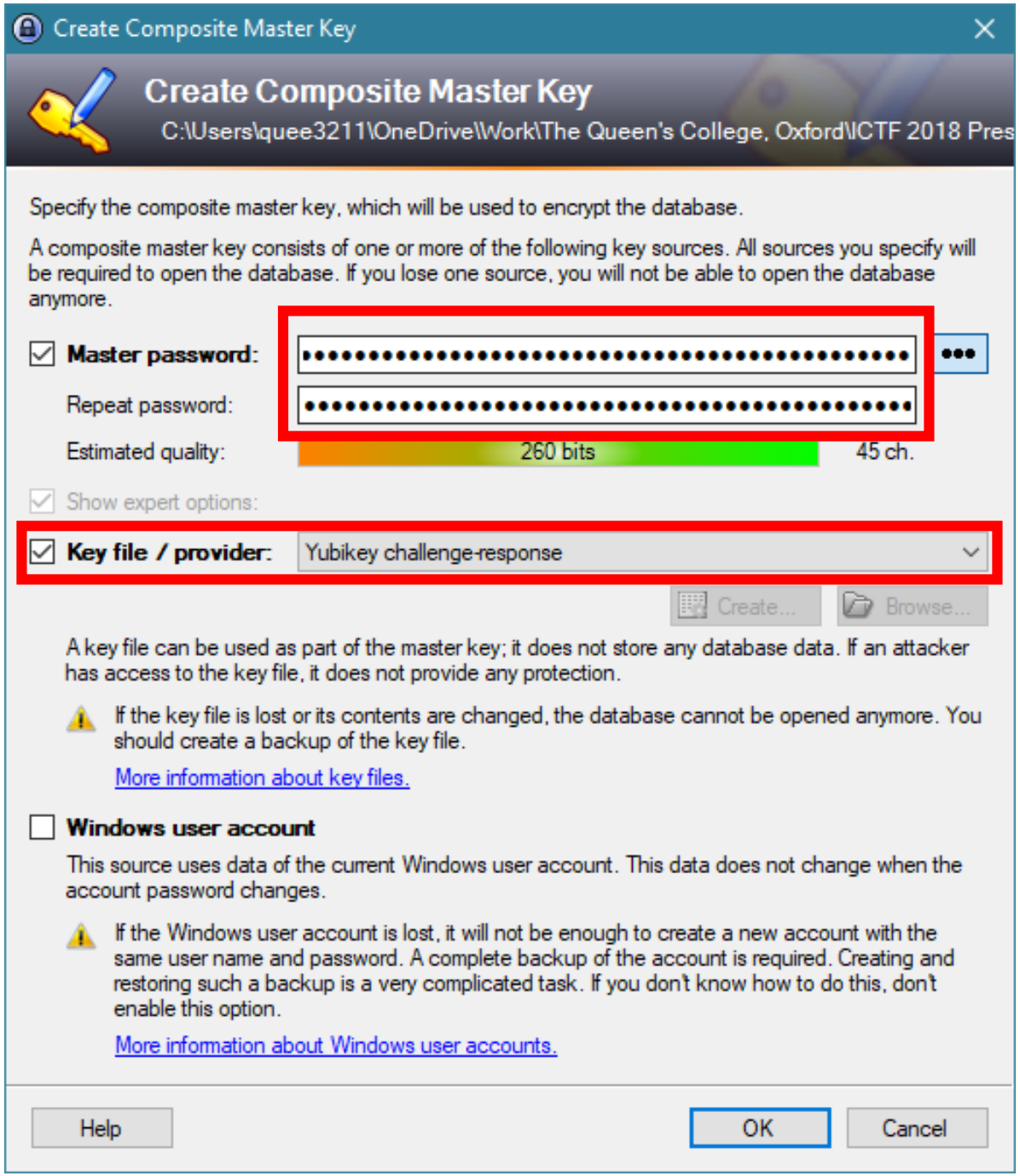

YubiKey Personalization Tool
Yubico OTP
OATH-HOTP
Static Password
Challenge-Response
Settings
Tools
About
Exit
Settings
General Settings
Decimal
ModHex
Hex
Use and enforce customer prefix
Output Settings
Output Format
Tab
Public ID
Tab
OTP
Tab
Enter
Output Speed Throttling
Output Character Rate
Standard
Add a short delay before sending OTP part
Add a short delay after sending OTP part
Serial # Visibility Settings
Button at startup (2.2+)
USB descriptor (2.2+/3.2+)
API call (2.2+/3.0+)
Static Password Settings
Enable manual update using the button (2.0+)
Extended Settings
Use numeric keypad for digits (2.3+)
Use fast triggering if only slot 1 is programmed (2.3+)
Invert led behaviour (2.4+/3.1+)
Update Settings
Enable updating of YubiKey configuration (2.3+/3.0+)
Log configuration output
Traditional format
Application Settings
Enable configuration export and import (experimental)
Actions
Settings are saved automatically
Restore Defaults
Update is available for YubiKey 2.3 and later
Update Settings...
YubiKey is inserted
Programming status:
Slot 1 and 2 configured
Firmware Version:
4.3.7
Serial Number
Dec: 7316790
Hex: 6fa536
Modhex: hvlgeh
Features Supported
Yubico OTP
2 Configurations
OATH-HOTP
Static Password
Scan Code Mode
Challenge-Response
Updatable
Ndef
Universal 2nd Factor
yubico

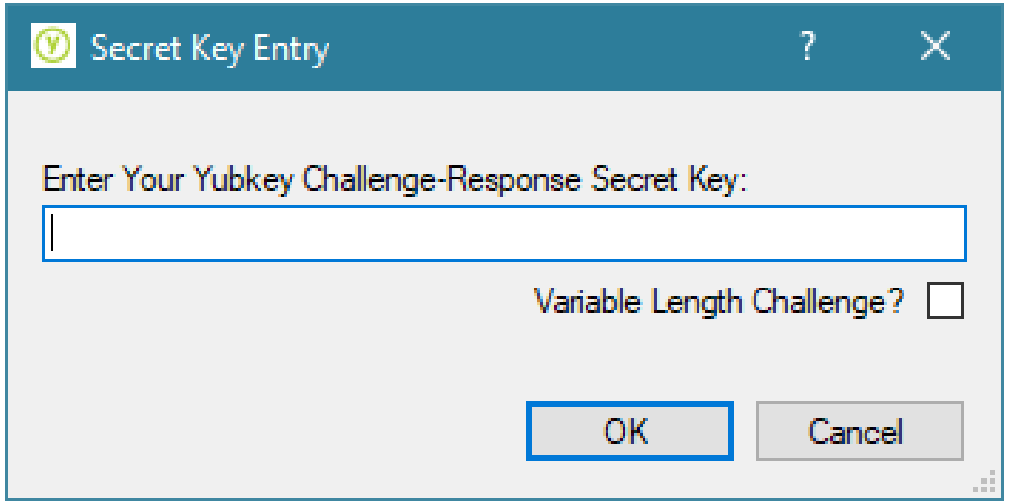




https://www.grc.com/passwords.htm


YubiKey Personalization Tool
Yubico OTP
OATH-HOTP
Static Password
Challenge-Response
Settings
Tools
About
Exit
Program in Challenge-Response mode
Yubico OTP
Allows you to program one or more YubiKeys in "Yubico OTP" Challenge-Response mode
HMAC-SHA1
Allows you to program one or more YubiKeys in "HMAC-SHA1" Challenge-Response mode
YubiKey is inserted
YubiKey Personalization Tool
Yubico OTP
OATH-HOTP
Static Password
Challenge-Response
Settings
Tools
About
Exit
Program in Challenge-Response mode - HMAC-SHA1
Configuration Slot
Select the configuration slot to be pro
Configuration Slot 1
Configuration Slot 2
Program Multiple YubiKeys
Automatically program YubiKeys when inserted
Parameter Generation Scheme
Randomize Secret
Configuration Protection (6 bytes Hex)
YubiKey(s) unprotected - Keep it that way
Current Access Code
Use Serial Number
New Access Code
Use Serial Number
HMAC-SHA1 Parameters
Require user input (button press)
HMAC-SHA1 Mode
Variable input
Fixed 64 byte input
Secret Key (20 bytes Hex)
aa 8c 2b 33 80 73 5f 24 2a 2d da 49 2e 37 65 cf a1 71 4
Generate
Actions
to program your YubiKey's selected configuration slot
Write Configuration
Stop
Reset
Back
Results
#
Status
Timestamp
YubiKey is inserted
Programming status:
Slot 1 and 2 configured
Firmware Version:
4.3.7
Serial Number
Dec: 7316790
Hex: 6fa536
Modhex: hvlgeh
Features Supported
Yubico OTP
2 Configurations
OATH-HOTP
Static Password
Scan Code Mode
Challenge-Response
Updatable
Ndef
Universal 2nd Factor
yubico


Create Composite Master Key
Create Composite Master Key
C:\Users\quee3211\OneDrive\Work\The Queen's College, Oxford\CTF 2018 Pres
Specify the composite master key, which will be used to encrypt the database.
A composite master key consists of one or more of the following key sources. All sources you specify will be required to open the database. If you lose one source, you will not be able to open the database anymore.
Master password:
Repeat password:
Estimated quality:
260 bits
45 ch.
Show expert options:
Key file / provider:
Yubikey challenge-response
Create...
Browse...
A key file can be used as part of the master key; it does not store any database data. If an attacker has access to the key file, it does not provide any protection.
If the key file is lost or its contents are changed, the database cannot be opened anymore. You should create a backup of the key file.
More information about key files.
Windows user account
This source uses data of the current Windows user account. This data does not change when the account password changes.
If the Windows user account is lost, it will not be enough to create a new account with the same user name and password. A complete backup of the account is required. Creating and restoring such a backup is a very complicated task. If you don't know how to do this, don't enable this option.
More information about Windows user accounts.
Help
OK
Cancel


Secret Key Entry
Enter Your Yubkey Challenge-Response Secret Key:
Variable Length Challenge?
OK
Cancel

Links

- Yubico Smart Card Deployment Guide - https://support.yubico.com/support/solutions/articles/15000006456-yubikey-smart-card-deployment-guide
- Yubico Smart Card Drivers - https://www.yubico.com/products/services-software/download/smart-card-drivers-tools/
- YubiKey Personalisation Tools - https://www.yubico.com/products/services-software/download/yubikey-personalization-tools/
- Resetting the Smart Card (PIV) Applet on Your YubiKey - https://support.yubico.com/support/solutions/articles/15000008587-resetting-the-smart-card-piv-applet-on-your-yubikey
- 5 fun applications to think about when deploying Smart Cards - https://myworldofit.net/?p=9509
- Yubikey on reddit - https://www.reddit.com/r/yubikey

Any Questions?