

Disk Encryption with the YubiKey and TrueCrypt

TrueCrypt and the YubiKey

Version: 1.0

Date: 28th April 2010

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

Trademarks

Yubico and YubiKey are trademarks of Yubico AB.

Contact Information

Yubico AB
Mäster Samuelsgatan 60, 8 floor
111 21 Stockholm
Sweden
info@yubico.com

Contents

1	Document Information	4
1.1	Purpose	4
1.2	Audience	4
1.3	Related documentation	4
1.4	Document History	4
1.5	Definitions	4
2	Introduction	5
3	Using the YubiKey in a Key strategy	6
4	Risks	7
5	Key Strategy	8
6	Programming the YubiKey	9
7	Encrypting a Laptop	12
8	Advanced topics	13
8.1	YubiKey configuration protection	13
8.2	Encryption Key file format	13
8.3	Bulk Programming	13
8.4	Costs	13
8.5	Windows Policy	13
9	End User Guide	14
10	Help Desk Topics	15
10.1	User forgotten their YubiKey – but it is still safe	15
10.2	User lost their YubiKey	15
10.3	User forgotten their password, but retains their YubiKey	15
10.4	User loses their Laptop	15
10.5	Security Administrators can help recover information	15

1 Document Information

1.1 Purpose

This document discusses the implementation of a pragmatic and simple scheme for full disk encryption on Windows Laptops using TrueCrypt Open Source Software and the YubiKey in static mode.

While Full Disk Encryption products look to integrate the more complex and robust "Challenge/Response" mode of the YubiKey, the methods discussed here are designed to allow an organisation to take immediate action on unencrypted Laptops which cover a number of risks.

1.2 Audience

ICT departments responsible for a number of Windows Laptops.

1.3 Related documentation

- YubiKey Personalization Tool – The Configuration Tool for the YubiKey
- The YubiKey Manual – Usage, configuration and introduction of basic YubiKey concepts
- TrueCrypt documentation <http://www.truecrypt.org/docs/>

1.4 Document History

Date	Version	Author	Activity
2010-03-120	0.1	JS	First draft

1.5 Definitions

Term	Definition
YubiKey device	Yubico's authentication device for connection to the USB port
USB	Universal Serial Bus
AES	Advanced Encryption Standard. A NIST approved symmetric encryption algorithm.
FDE	Full Disk Encryption
OTP	One Time Passcode – the default mode for a YubiKey is to generate OTPs.
TrueCrypt	A free open source software for encryption of computer files and disks.

2 Introduction

TrueCrypt is free open-source disk encryption software for Windows 7/Vista/XP and other operating systems. It has the capability to create a virtual encrypted disk within a file and mount it as a real disk. It also has the capability to encrypt a system drive where Windows is installed – requiring pre-boot authentication.

When an organisation loses a Laptop, not only is the physical asset lost but potentially significant amounts of data stored on the hard disk on the Laptop is lost too. Whereas the cost of losing the physical asset is known, the loss of data is often much greater if it falls into the hands of the wrong party.

Encrypting the whole disk (Full Disk Encryption – FDE) on a Laptop is often recommended over file encryption as it eliminates the chance non-encrypted data is lost. Therefore, this document will focus on...

Encryption applies mathematical algorithms to data before it is stored; this process is reversible if the user knows the key. If a good algorithm is used and the key is “strong”, it is infeasible for someone without the key to reverse the process – and the resulting data appears to be random noise.

It is beyond the scope of this document to discuss further “good” algorithms for encryption. However, TrueCrypt by default uses AES which is considered to be a good military strength algorithm to which a key of at least 128bits needs to be applied in order to be considered sufficiently strong.

Use of a strong key is a significant issue which this document discusses in detail.

3 Using the YubiKey in a Key strategy

The YubiKey is a USB device which presents itself to a computer as a Human Interface Device – HID – a keyboard. It is a 3 gram hermetically sealed keyboard with a single key – actually a touch button.



Both sides of a YubiKey.

The YubiKey was designed to be used to generate securely encrypted One Time Passcodes (OTP). However, it is also able to program the YubiKey to emit a static string of characters – which is the capability used in this document.

4 Risks

Effective disk encryption relies on the “key” being kept secret from the potential thief.

If Full Disk Encryption is employed with a good algorithm and a strong key which has been kept secret, it is thought all data on the hard drive of the Laptop will appear as just noise.

The strategy described in this document assumes the YubiKey used to store part of the “key” and the contents of that key are not given up to the thief with the Laptop. If the Thief has the YubiKey and the Laptop, the security is much diminished. Therefore, users of Laptops using the method described in this document must be trained to keep their YubiKey safe and never left with the Laptop. We recommend instructing employees to put the YubiKey on their key ring with their house keys, and never in their Laptop bag. Furthermore, we recommend that the YubiKey is only ever inserted into the Laptop in the pre-boot environment, and is removed and securely stored once Windows starts to boot/restore from hibernation.

Where this level of security is not sufficient, organisations may consider deploying the YubiKey with supported commercial software in the Challenge/Response mode – this is outside the scope of this document. For further security, a smartcard solution may be considered.

5 Key Strategy

The YubiKey can be programmed to emit a string of up to 64 characters. A strong key is often considered one which has 128 bits of length (or more) and with high entropy – or randomness.

As an HID device (keyboard), the YubiKey actually emits “scan codes” rather than actual characters. Different keyboard layouts have a different mapping between scan codes and the characters they represent. Therefore, Yubico has designed a character set which is invariant between keyboard layouts which has 16 characters and we call the Modhex set – Modified Hexadecimal. Therefore, each character has 4 bits of entropy. To get 128 bits key length, we recommend a static key of 32 characters. An example could be:

```
rcltrcihbkkiulnveuenervidliliiifv
```

For some additional security, we recommend the encryption key is made up of a short password known to the user plus the YubiKeys static output. For example:

```
Sunny33rcltrcihbkkiulnveuenervidliliiifv
```

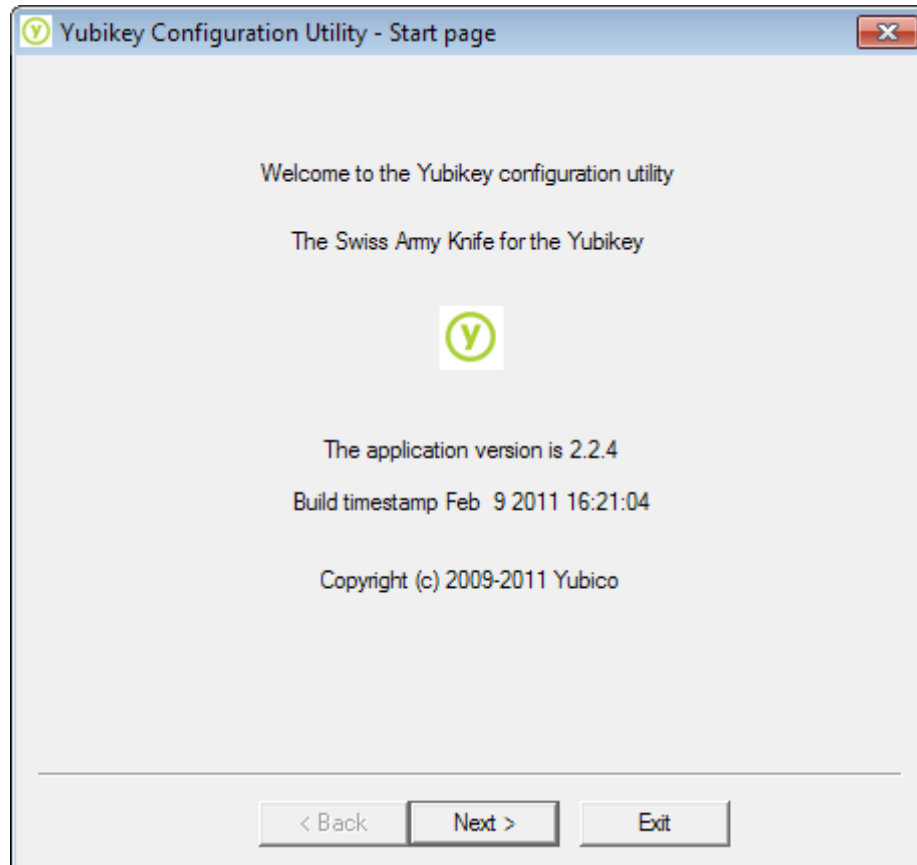
Where “Sunny33” is the users password.

6 Programming the YubiKey

Download the YubiKey Personalization tool v2.2.4 or later from

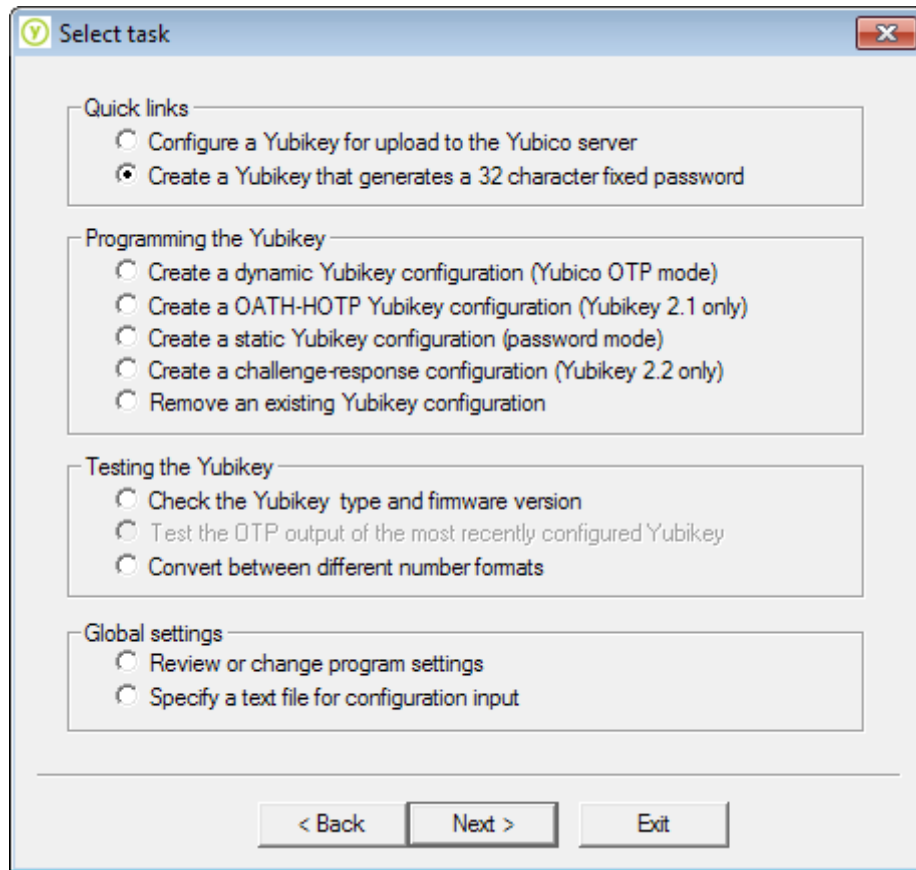
<http://www.yubico.com/personalization-tool>

Run the Program as check the splash screen:



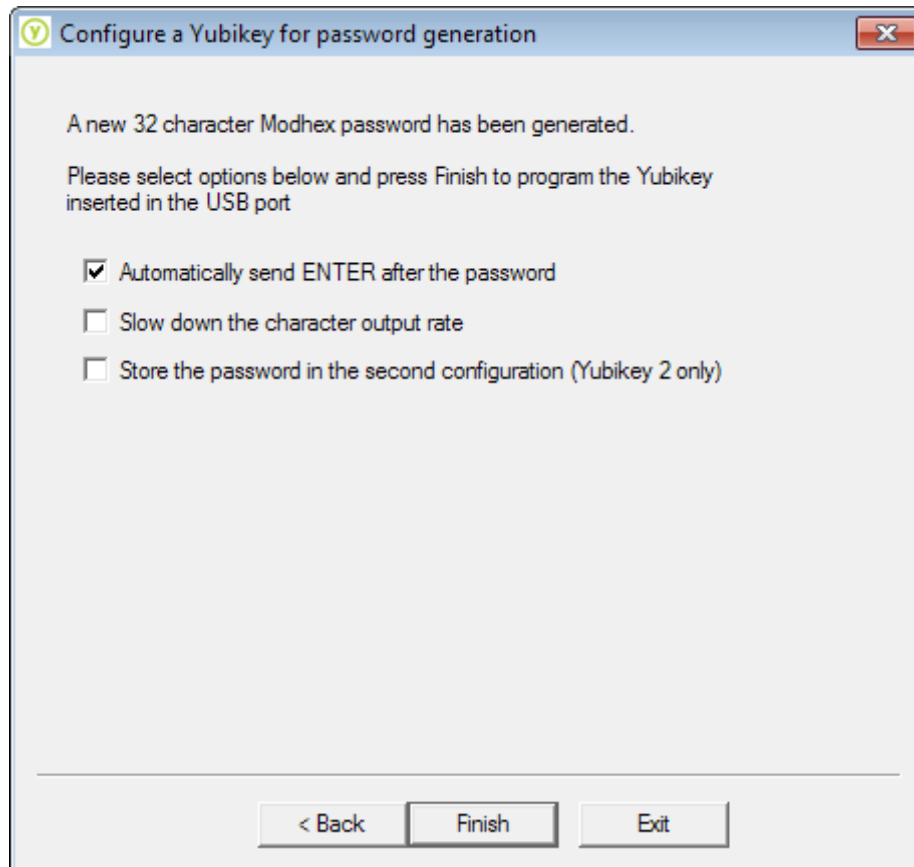
Press the "Next>" button.

yubico



Select the "Create a Yubikey that generates a 32 character fixed password" option in the "Quick links" group and press "Next>".

yubico



Make sure the "Automatically send ENTER after the password" option is selected and the other 2 options are not selected. Insert the next YubiKey into your USB port and press "Finish". The YubiKey will be programmed with a random static modhex password like:

```
rc1trcihbkkiulnveuenervidliliifv
```

Create or Open the YubiKey Static Password log file and record the static password against its serial number lasered on the reverse of the key. The management of this database is outside the scope of this document.

Continue to program the rest of the YubiKeys. When all YubiKeys required are programmed, press "Exit" to exit the personalization tool.

7 Encrypting a Laptop

Although the details of this procedure are outside the scope of this document, when using TrueCrypt to encrypt the Laptop you will need to enter an encryption key. Take the next YubiKey from your stock, and record its serial number together the Laptop asset tag and the name of the person the Laptop will be issued to.

When TrueCrypt asks for an encryption key, generate a random user password (e.g. "Sunny33" – though generation of these is outside the scope of this document), enter this and then insert the YubiKey into a USB port, and when the green dot is glowing steadily, touch the gold disc to emit the YubiKey's static 32 character password. As it also emits a ENTER character, TrueCrypt will automatically advance to the next stage.

8 Advanced topics

8.1 YubiKey configuration protection

Organizations may want to consider applying a configuration password to the YubiKeys to prevent the end user from reconfiguring their YubiKey. This is described in the Personalization Guide user manual which is available from:

<http://www.yubico.com/personalization-tool>

The YubiKey configuration is write only by design. If a new configuration is written the previous configuration is securely deleted.

8.2 Encryption Key file format

An example file format for storing encryption keys:

**Username, laptop asset tag, YubiKey serial number,
users password, YubiKey static password,
configuration password**

```
"JohnSalter", "X2973", 508436, "Sunny33",  
rcltrcihbkkiulnveuenervidliliifv, 0
```

Clearly the integrity and security of this file or database is critical to the security of encrypted Laptops. It is outside the scope of this document to make recommendations.

A zero configuration password indicates the password is not set.

8.3 Bulk Programming

Large orders of YubiKeys (500+) can be pre-configured to the organizations own specification and securely supplied with a secrets file

8.4 Costs

TrueCrypt is free open source software. The YubiKey personalization tools are free software and the personalization API is public domain with free open source libraries available at Google Code.

The YubiKey is sold by Yubico and pricing is supplied on request.

ICT Support teams will need to be trained in encrypting Laptops and programming Yubikeys.

8.5 Windows Policy

It is recommended organizations consider disabling the ability to "Sleep" a Laptop - as the encryption keys are maintained in memory when a Laptop is in "Sleep" mode. When a Laptop is in Hibernate or Power Off mode for more than a few minutes, the encryption keys are no longer in memory.

It may be wise to set a policy where the Laptop automatically hibernates when the Laptop lid is closed or the battery level falls below the low threshold.

9 End User Guide

When a Laptop is issued to the end user, they are also issued in unison with the YubiKey programmed with a random static 32 Modhex character password and are told their "prefix" password e.g. "Sunny33".

They are instructed to keep their YubiKey safe and never with their Laptop – maybe on the house key ring, or in their purse or wallet.

When they boot their Laptop they will be presented with the TrueCrypt boot loaded prompt:

```
TrueCrypt Boot Loader 7.0a

Keyboard Controls:
[Esc] Skip Authentication (Boot Manager)

Enter password:
```

They are instructed to enter their password (Sunny33 in this example), insert their YubiKey into a free USB port, wait for the green dot to steadily glow green and then to touch the gold disc. This will emit the static password (with an ENTER key at the end), and the Laptop should begin to boot into Windows (or to Restore if it was previously set into a hibernate state). The YubiKey should be immediately removed once Windows is starting. The YubiKey should never be inserted into the computer at any other time.

10 Help Desk Topics

10.1 User forgotten their YubiKey – but it is still safe

Instruct the user to enter their secret password and then dictate the password instructing the user to enter the characters in lowercase as dictated and not to write them down.

10.2 User lost their YubiKey

Require that the Laptop is returned to ICT for TrueCrypt to be updated with a new encryption key and a new YubiKey issued. The user's password may be retained.

10.3 User forgotten their password, but retains their YubiKey

Once the user is authenticated, remind the user of their password

10.4 User loses their Laptop

Ask user whether they have also lost their YubiKey? If not, the YubiKey must be securely returned to ICT for re-programming or to be destroyed. If they have, a potential data loss risk assessment should be made.

10.5 Security Administrators can help recover information

Security administrators may retain the list of the encryption keys for TrueCrypt for each user programmed into the Yubikeys so that in case a user lose their Yubikey or if the user is dismissed for any reason, then the administrator can help to recover the information.

In addition it is recommended that the password to store the encrypted list is divided in two halves where two administrators both have to submit their half (which again can be combined with using a Yubikey) to decrypt the file.