

## Background

The YubiKey 2.0 contains two completely independent configuration slots. If configuration slot 1 is changed it does not affect the configuration slot 2 and vice versa.

If the OTP is generated by pressing the YubiKey button for 0.3 to 1.5 seconds, the output (OTP or Static PW) will be coming from configuration slot 1 and if the YubiKey button is pressed for 2.5 to 5 seconds, then the output (OTP or Static PW) will be coming based on settings in configuration slot 2.

By default, when Yubico ships the YubiKey the configuration slot 1 is set to OTP mode and the second configuration slot is open to be set by the customer. You can for example set the configuration slot 2 for generating a static password. This way you can have a YubiKey generating both an OTP and a static password.

## Dynamic Configuration

By default, (when Yubico ships the YubiKey) the configuration slot 1 is set to OTP mode and working with the public Yubico Online validation service and the public identity, private identity and AES Key values are all stored within the Yubico Online validation service. Users can validate the OTP generated from the YubiKey as soon as they receive the YubiKey. The second configuration slot is not configured by default and is therefore open to be set by the customer.

Please note that, re-initializing of YubiKey configuration slot 1 (either by manually programming a new AES key in any of the configuration of the YubiKey or programming the any of the configuration of the YubiKey for static PW), you will lose ALL abilities to validate the OTP generated from that particular configuration of the YubiKey against Yubico online validation server, thus losing all abilities to use that particular YubiKey with any of Yubico online servers for which you have enrolled for example Yubico forum, demo server, OpenID server and so on.

In order to streamline the process for users who want to program their own AES keys in YubiKeys and still have a working YubiKey online we have changed the process of handling AES Keys at the online validation server. You will have to use a YubiKey configuration utility to program your own AES keys into a YubiKey and then upload the same AES key(s) to the server (to be used online) using the following link:

<http://www.yubico.com/developers/aeskeys/>

For more information about reconfiguration or uploading the AES Key, please see the YubiKey Configuration Manual.

## Uploading AES Key

In order to streamline the process for users wanting to program their own AES keys into their YubiKeys and still have a working YubiKey for Online validation we have changed the process of handling AES Keys for the Yubico Online validation server.

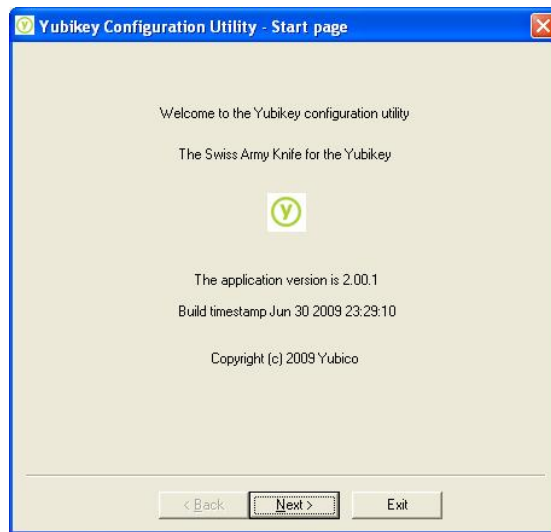
Users will now use the YubiKey configuration utility to program their own AES key into a YubiKey and then upload the AES key(s) to the server (in order for a YubiKey to be used online). The keys are uploaded using the following link:

<http://www.yubico.com/developers/aeskeys/>

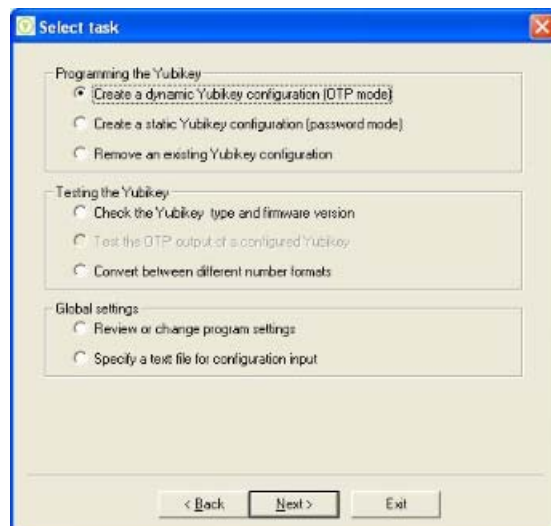
The following steps explain how to program and upload the AES Key in order to have access to the AES key in the Yubikey and then how to once again be validating the YubiKey OTP with the Online Yubico validation server through uploading the key to the Yubico online validation server:

Customers should be informed it will take at least 4 weeks to schedule the production of this option as it requires special handling at the personalisation stage and cannot be provided for from stocks.

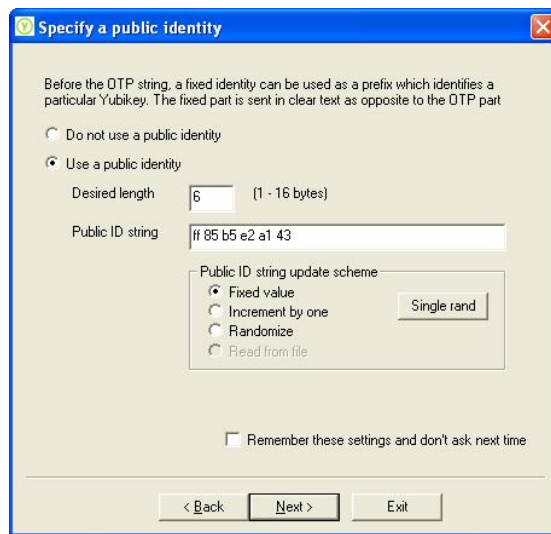
1. Start the YubiKey configuration utility



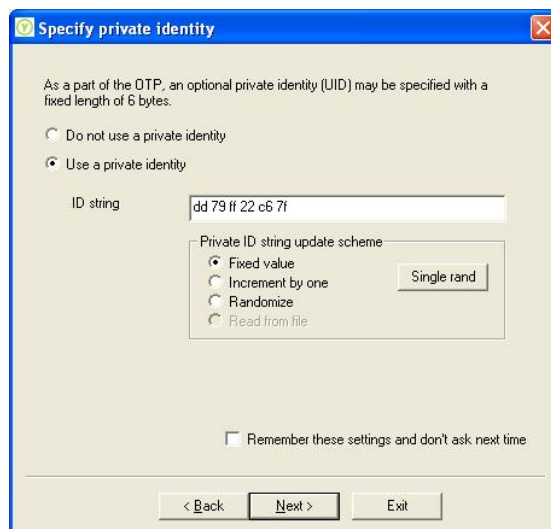
2. From the "Select task" screen, select "Create a dynamic YubiKey configuration(OTP mode)" from "Programming the YubiKey" section



3. Select "Use a public identity" and set the desired length to 6 (i.e. 6 full hex values or 12 individual hex characters). The AES Key upload functionality requires the YubiKey Public ID aka public identity (first 12 modhex characters of the OTP also known as YubiKey prefix) to start with "vv". To achieve this, please reprogram your YubiKey with the Public ID to start with "ff". For example, the YubiKey programmed with the Public ID " ff85b5e2a143" will generate a OTP with "vvjngudlbfe" prefix.  
There is a conversion calculator available on the Yubico web site to help convert between hex and modhex formats.



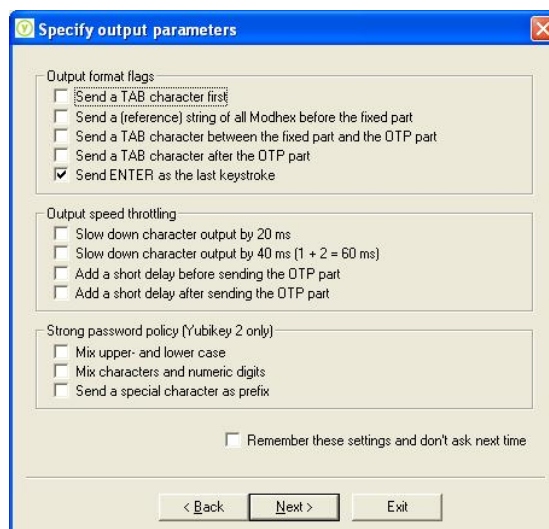
4. Select "Use a private identity" and enter the desired value in hex encoded format. Note down the selected hex encoded value as it is required while uploading the AES Key.



5. Select the desired AES Key and enter it in hex encoded format. Please make sure to note down the selected hex encoded value as it is required input when uploading the AES Key a bit later in the process.

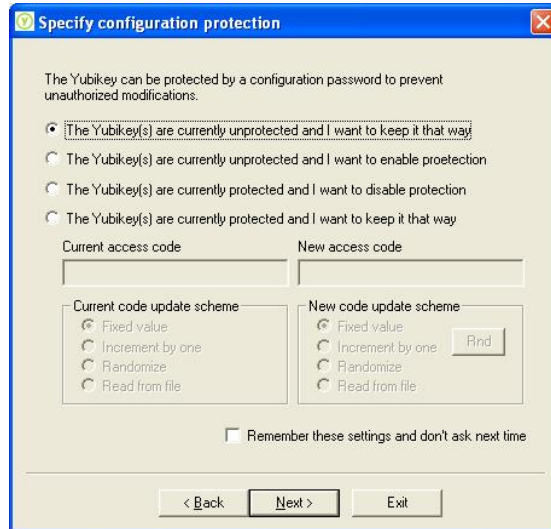


6. Do not select the following options from "Specify output parameters" screen if you want to validate the OTP with the online Yubico validation server. All other options are optional.



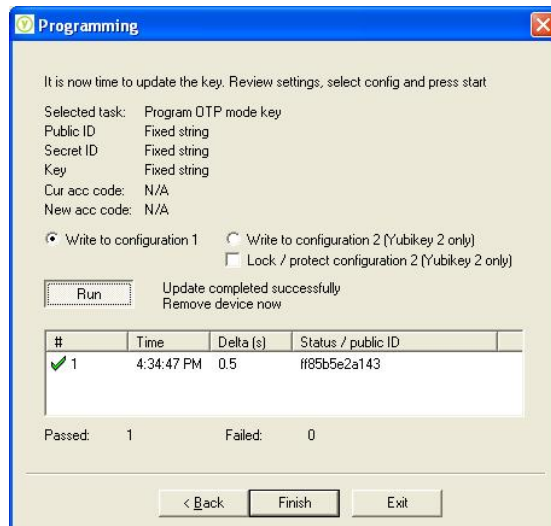
- Send a TAB Character first
- Send a (reference) string of all Modhex characters before the fixed part
- Send a TAB character between the fixed part and the OTP part
- Send a TAB character after the OTP part
- Add a short delay before sending the OTP part
- Add a short delay after sending the OTP part
- Mix upper- and lower case
- Mix characters and numeric digits
- Send a special character as prefix

- Specify a configuration change protection password if you want or if you have already set the password, it will be shown in the screen.



- From the "Programming", select the "Write to configuration 1" if you want to change the configuration 1 to OTP mode or " Write to configuration 2 (for YubiKey 2.x versions only)" option if you want to change the configuration 2 to OTP mode and click on "Run".

Note: that writing only to configuration 2 will preserve configuration 1 intact so that you can use the original OTP with the Online Validation Server without uploading configuration 2 to the Yubico online server.



- 9. Once, the YubiKey has been reprogrammed, we need to upload the information using the following link:

<http://www.yubico.com/developers/aeskeys/>

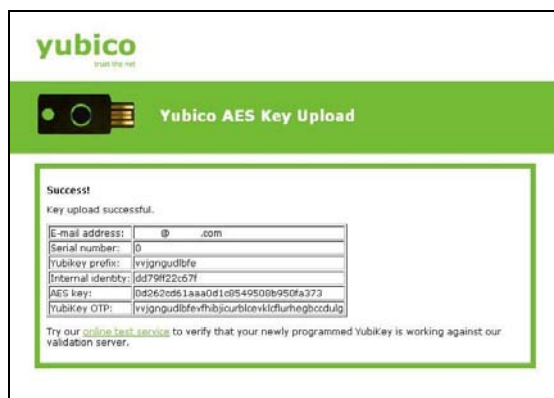
The AES Key upload page is shown below:



- 10. Information about each YubiKey are filled out as shown in the example below:



11. The following screen is shown once the AES Key and other information is uploaded successfully:



12. Now the OTP can be validated again with the with the online Yubico validation server.

Document Details
Author: Kurt Lennartsson
Date of release: 15 <sup>th</sup> September 2009
Version: V2.0
Valid from: Immediate
Valid to: 31 <sup>st</sup> December 2009