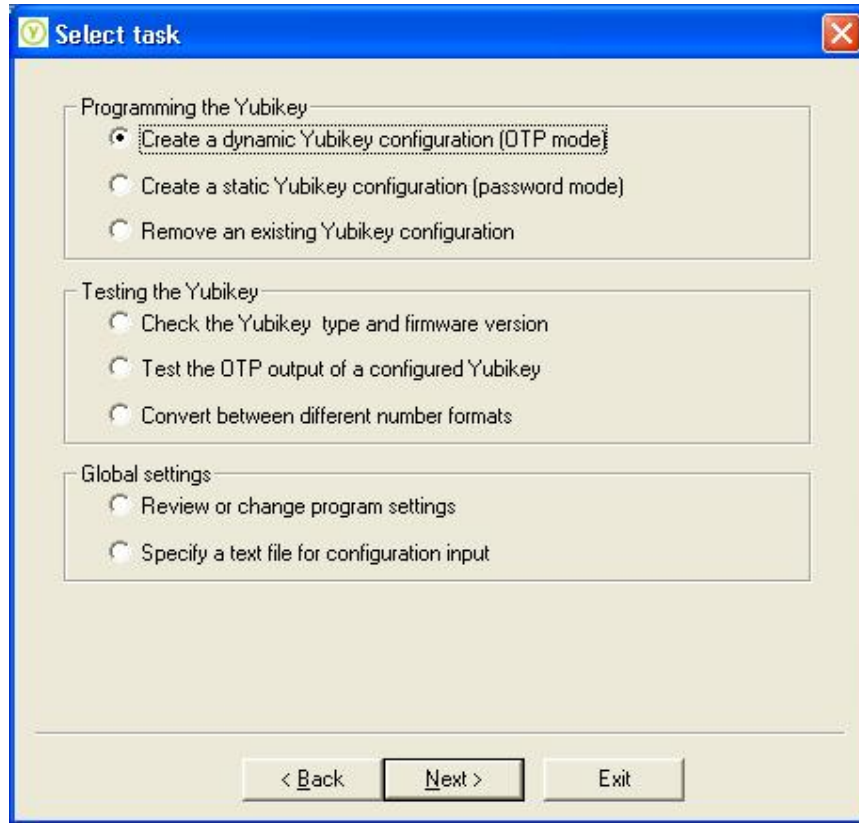


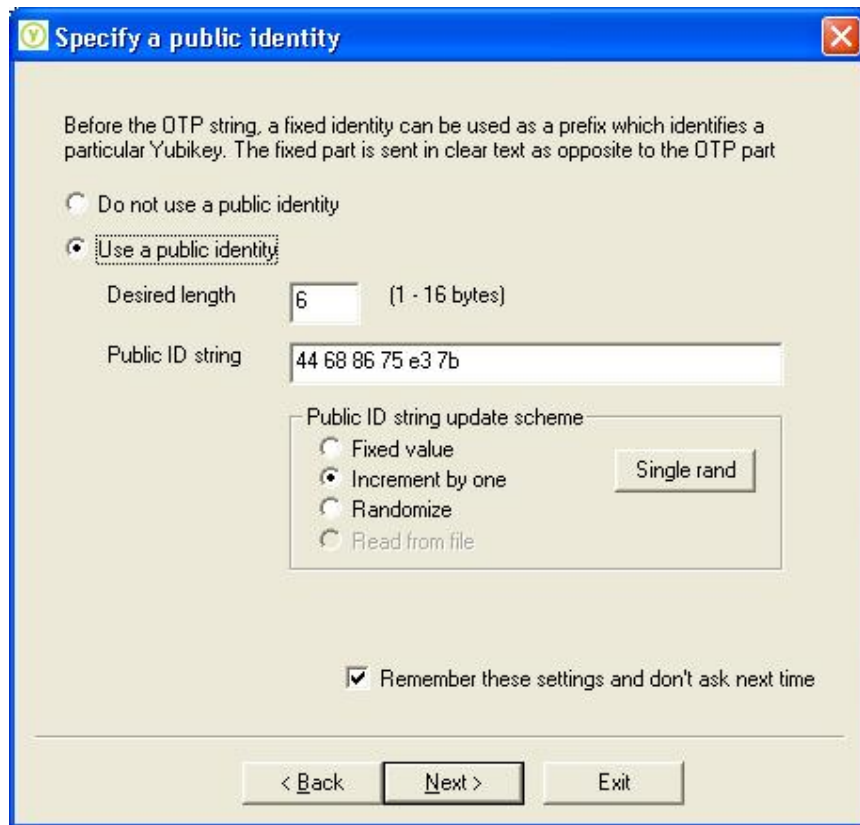
# Yubikey. Setup Dynamic configuration for Rohos Logon with static AES

Comments are below each picture.



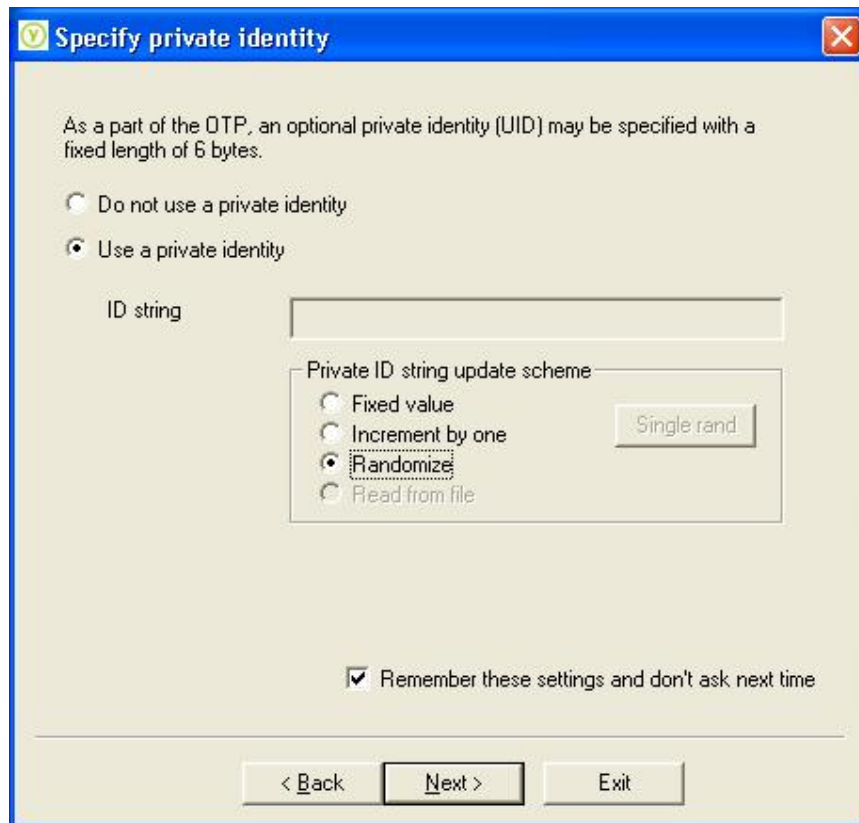
We need to Set up Dynamic configuration (OTP).

The following configuration would be OK for login by Yubikey to Windows Remote Desktop by Rohos.



6 bytes for public identify. Required by Rohos. Please see Yubico PDF about this identify for acknowledge.

Click "Single rand" and then "Increment by one" or "Randomize". These values are always visible in OTP. They should not be remembered.



Private identify is not used by Rohos. (But it should be 6 bytes length just in case).

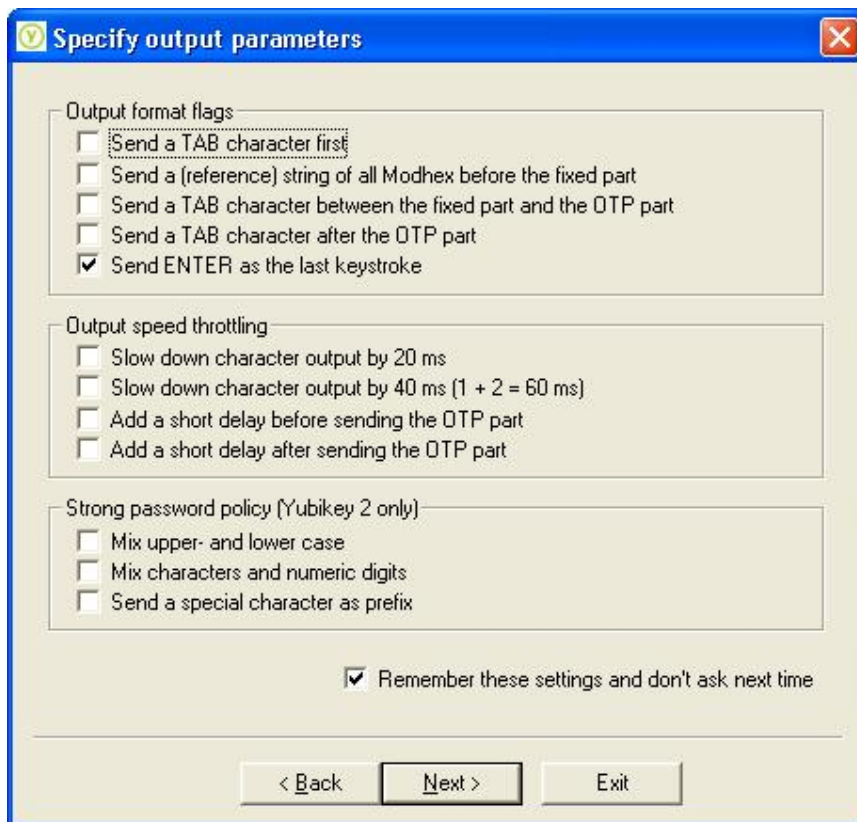


AES key is important part. Click “Fixed” and then “Single Rand”. Remember this AES key you will need to enter into Rohos later.

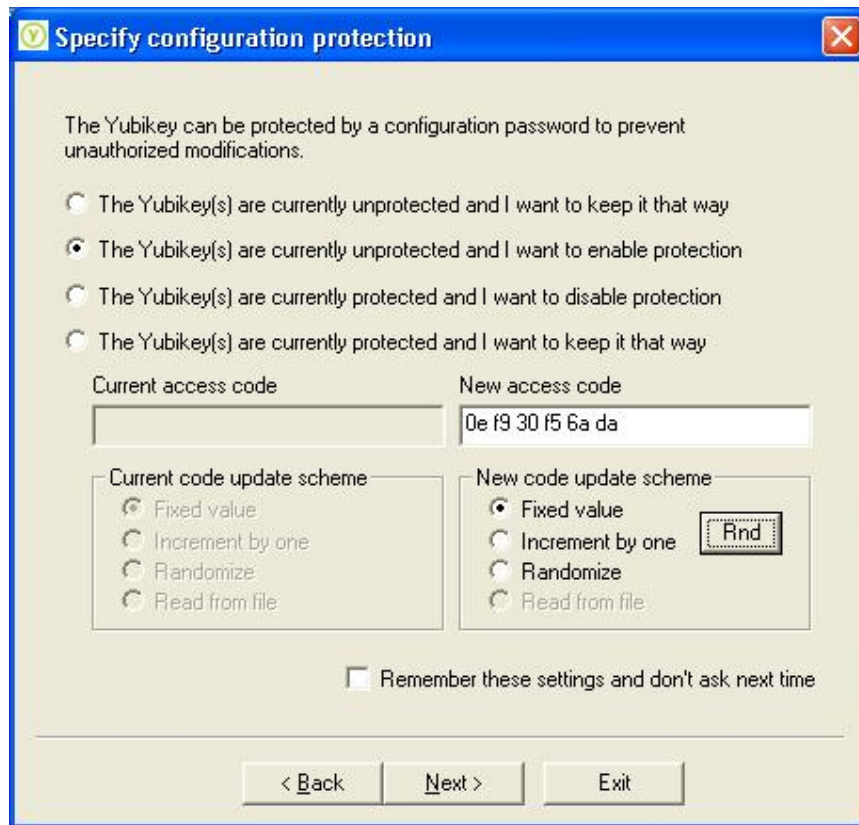
Rohos may authenticate Yubikey by...

- by using a single (fixed) AES key that you need to enter in Rohos. That is why I set “Fixed value” on the screen.
- by using a URL of a validation server (Yubico by default) but in this case you will need to import all generated AES keys + Public identify of the tokens into Yubico validation server.

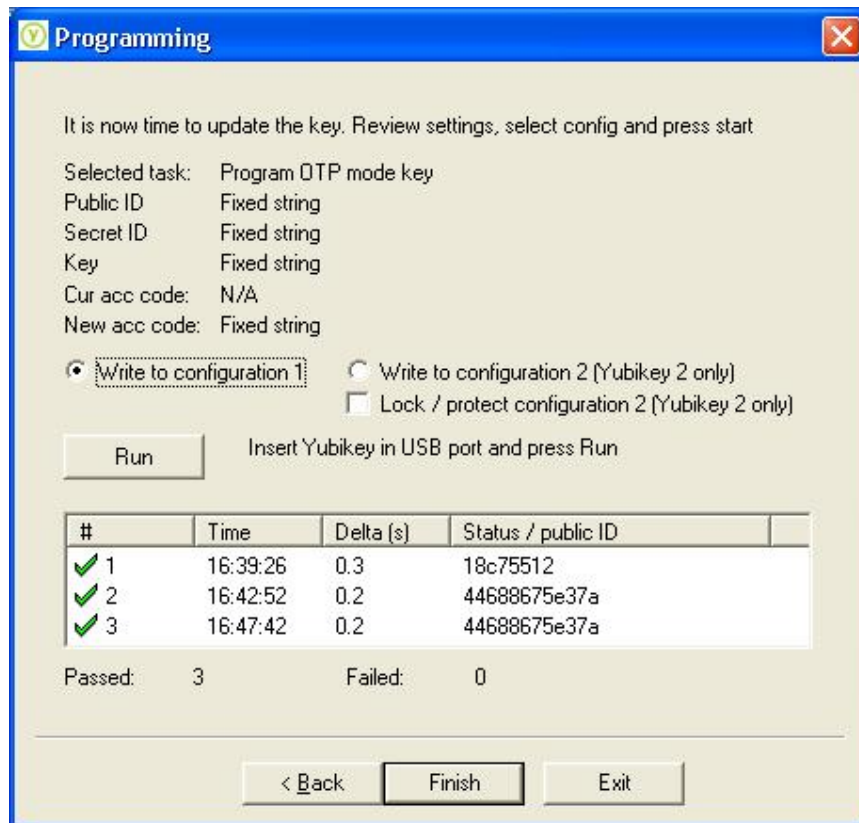
As we don't know how to do it right now we do not use the option.



No comments.



We suggest protecting Yubikey against unauthorized re-configuration. Click a RND and set it Fixed.  
**Remember this value**



This is the final.

Remove any Yubikey.

“Write configuration 1” selected.

Click on Run.

- Connect Yubikey 1.
- Remove Yubikey 1
- Connect Yubikey 2
- Remove Yubikey 2
- ..

Test the keys. They should produce the following OTP (44 bytes):

```
ffhjjhigueilkubigcienvcrbtgtgelvtrcjubftcgud
ffhjjhigueilfbnhkbhntjctfdttgleiunlrbgjurdk
ffhjjhigueilfdgjjitdcgdkurfhejjbdlitubrdbkk
ffhjjhigueilueetivhnnukbricktcvdkdbtvngtfetb
ffhjjhigueillkblketerkvddivnkfkrgehjdejvgcej
```

as you see first 12 chars are Yubikey ID then OTP.