NAME

ykchalresp − Perform challenge−response operation with YubiKey

SYNOPSIS

ykchalresp [*−nkey*] [*−1* | *−2*] [*−H* | *−Y*] [*−N*] [*−x*] [*−v*] [*−6* | *−8*] [*−t*] [*−iFILE*] [*−V*] [*−h*]

DESCRIPTION

Send a challenge to a YubiKey, and read the response. The YubiKey can be configured with two different C/R modes — the standard one is a 160 bits HMAC−SHA1, and the other is a YubiKey OTP mimicking mode, meaning two subsequent calls with the same challenge will result in different responses.

OPTIONS

−nkey

send the challenge to the nth key found.

−1

send the challenge to slot 1. This is the default

−2

send the challenge to slot 2.

−H

send a 64 byte HMAC challenge. This is the default.

−Y

send a 6 byte Yubico OTP challenge.

−N

non−blocking mode — abort if the YubiKey is configured to require a key press before sending the response.

−x

challenge is hex encoded.

−v

enable verbose mode.

−6

output the response in OATH format, 6 digits.

−8

output the response in OATH format, 8 digits.

−t

use current time as challenge instead of reading challenge from command line (as in default TOTP mode, seconds since 1970−01−01 00:00:00 / 30 encoded as an 8 byte challenge).

−i*FILE*

take challenge from FILE instead of as an argument. If file is − challenge is read from STDIN

−V

print tool version and exit.

EXAMPLE

The YubiKey challenge−response operation can be demonstrated using the **NIST PUB 198 A.2** test vector.

First, program a YubiKey with the test vector :

```
$ ykpersonalize −2 −ochal−resp −ochal−hmac −ohmac−lt64 −a303132333435363738393a3b3c3d3e3f40414243
 ...
Commit? (y/n) [n]: y
$
```

Now, send the NIST test challenge to the YubiKey and verify the result matches the expected :

```
$ ykchalresp −2 'Sample #2'
0922d3405faa3d194f82a45830737d5cc6c75d24
$
```

BUGS

Report ykchalresp bugs in the issue tracker https://github.com/Yubico/yubikey−personalization/issues

SEE ALSO

The ykpersonalize home page https://developers.yubico.com/yubikey−personalization/

YubiKeys can be obtained from Yubico http://www.yubico.com/