Software Signing

Yubico aims to cryptographically sign all software that it distributes. We use three different techniques to achieve this.

OpenPGP Software Signing

Source code releases are usually signed by an OpenPGP key of one of Yubico's developers. Some ZIP files containing Windows executables are also signed using OpenPGP.

Following are the keys for Yubico developers who are currently releasing code.

- Klas Lindfors <klas@yubico.com> 0A3B 0262 BCA1 7053 07D5 FF06 BCA0 0FD4 B216 8C0A
- Dain Nilsson <dain@yubico.com> 20EE 325B 86A8 1BCB D3E5 6798 F043 6709 6FBA 95E8
- Alessio Di Mauro <alessio@yubico.com> B70D 62AA 6A31 AD6B 9E4F 9F4B DC88 8892 5D25 CA7A
- Tommaso De Orchi <tom@yubico.com> FF8A F719 AE58 2818 1B89 4D83 1CE3 9268 A097 3948
- Jean Paul Galea <jeanpaul@yubico.com> B604 2E2B D1FD BC2B CA85 88B2 FF8D 3B45 B7B8 75A9
- Emil Lundberg <emil@yubico.com> 57A9 DEED 4C6D 962A 923B B691 816F 3ED9 9921 835E
- Trevor Bentley <trevor@yubico.com> 2685 83B6 4786 F50F 8074 56DA 8CED 3A80 D41C 0DCB
- Aveen Ismail <aveen.ismail@yubico.com> 1D73 08B0 055F 5AEF 3694 4A8F 27A9 C24D 9588 EA0F
- Alessandro Carlo Chirico <alessandro.chirico@yubico.com> 355C 8C01 86CC 96CB A49F 9CD8 DAA1 7C29 5391 4D9D
- Dennis Fokin <dennis.fokin@yubico.com> 9E88 5C03 02F9 BB91 6752 9C2D 5CBA 11E6 ADC7 BCD1
- Konstantinos Georgantas <kostas@yubico.com> 7FBB 6186 9574 96D5 8C75 1AC2 0E77 7DD8 5755 AA4A
- Ludvig Michaelsson <ludvig.michaelsson@yubico.com> 78D9 97D5 3E9C 0A2A 2053 92ED 14A1 9784 723C 9988
- Adam Velebil <adam.velebil@yubico.com> AF51 1D2C BC0F 973E 5D30 8054 325C 8E4A E2E6 437D

Following are the keys for developers who have released code in the past.

- Dag Heyman <dag@yubico.com> 8D0B 4EBA 9345 254B CEC0 E843 514F 078F F4AB 24C3
- Nigel Williams <nigel.williams@yubico.com> 1DC4 BA28 7252 5B3F 2FE8 207F 5D9C 760A 3FB5 1707
- Simon Josefsson <simon@yubico.com> 9AA9 BDB1 1BB1 B99A 2128 5A33 0664 A769 5426 5E8C
- Henrik Stråth <henrik@yubico.com> DCB9 04FA B343 CFA7 1907 6EF7 9EA9 0242 958E 0658

- Pedro Martelletto <pedro@yubico.com> `EE90 AE0D 1977 4C83 8662 8FAA B428 949E F791 4718`

Verifying signatures with GnuPG

The list above lists primary key fingerprints, but GnuPG may print a subkey fingerprint if you attempt to verify a signature made with an unknown key. You can use `gpg --recv-keys` to download the necessary key.

Caution Regardless of how you download keys, you must always verify that signatures were made by one of the keys listed above. See below for an example of how to to this.

Example of downloading key by subkey ID:

```
$ gpg --verify yubioath-desktop-5.0.5.tar.gz.sig
gpg: assuming signed data in 'yubioath-desktop-5.0.5.tar.gz'
gpg: Signature made tor 15 apr 2021 16:23:47 CEST
gpg:                using RSA key D6919FBF48C484F3CB7B71CD870B88256690D8BC
gpg: Can't check signature: No public key

$ gpg --recv-keys D6919FBF48C484F3CB7B71CD870B88256690D8BC
gpg: key 5CBA11E6ADC7BCD1: public key "Dennis Fokin <dennis.fokin@yubico.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Example of verifying signature:

```
$ gpg --verify yubioath-desktop-5.0.5.tar.gz.sig
gpg: assuming signed data in 'yubioath-desktop-5.0.5.tar.gz'
gpg: Signature made tor 15 apr 2021 16:23:47 CEST
gpg:                using RSA key D6919FBF48C484F3CB7B71CD870B88256690D8BC
gpg: Good signature from "Dennis Fokin <dennis.fokin@yubico.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 9E88 5C03 02F9 BB91 6752  9C2D 5CBA 11E6 ADC7 BCD1
     Subkey fingerprint: D691 9FBF 48C4 84F3 CB7B  71CD 870B 8825 6690 D8BC
```

Make sure that gpg reports `Good signature` **AND** that the `Primary key fingerprint` is listed above. You can safely ignore the warning `key is not certified with a trusted signature` if you have manually verified the primary key fingerprint.

Windows Software Signing

Our Windows executables are signed with one of the following code signing certificates, issued by DigiCert:

yubico-windows-code-ev-current.pem

SHA256 Fingerprint `33:25:6D:85:EE:41:F6:DF:D7:92:3B:AC:16:EC:E9:9F:98:CB:D6:A8:9D:71:90:CE:06:31:1A:68:55:A4:DA:67`

yubico-windows-code-ec-current.pem

SHA256 Fingerprint `EC:BF:1B:DA:58:17:48:1C:51:FA:E7:B8:BD:FA:4C:09:A8:26:BB:05:05:8D:13:0D:34:32:2E:A1:94:C7:73:07`

yubico-windows-code-rsa-current.pem

SHA256 Fingerprint `A0:1E:11:73:E5:15:18:09:53:8D:FD:24:92:D5:C2:91:DB:F4:EC:67:B5:A5:CF:06:13:71:98:5E:34:36:5D:E6`

Earlier Windows software may be signed with one of the following certificates:

yubico-windows-code-ev-2020.pem

SHA256 Fingerprint `D3:E2:EF:AA:70:13:B1:79:2D:E4:84:90:26:50:FC:A1:1D:69:60:DE:77:FD:8C:8E:BB:37:3F:A8:68:8B:33:7F`

yubico-windows-code-2021.pem

SHA256 Fingerprint `C9:E7:75:63:0C:3E:F9:DB:02:7C:78:80:2C:0D:BD:E0:93:F5:38:CE:64:7A:C0:EF:25:8C:F4:86:94:F5:CD:DB`

yubico-windows-code-ev-2017.pem

SHA256 `C3:C1:BE:40:B7:F2:C7:B2:51:DB:67:35:88:40:76:9F:37:35:28:D2:5E:32:AD:0D:80:6F:01:C6:ED:96:E8:2D` fingerprint

yubico-windows-code-2018.pem

SHA256 `43:9D:B8:FB:32:F3:BA:47:15:5C:BA:E5:8A:02:A5:02:B3:ED:15:7A:34:23:B8:62:74:6E:20:AE:17:7F:5C:ED` fingerprint

yubico-windows-code-2017.pem

SHA256 `42:77:C7:17:01:5F:DB:6F:EA:CC:5D:4B:69:BD:72:D7:64:18:3E:6A:81:D6:64:87:BC:70:E9:B6:C5:9C:01:FE` fingerprint

yubico-windows-code-2016.pem

SHA256 `F0:45:D8:A2:54:37:97:B1:29:6F:32:A1:4F:6C:BC:C6:13:5F:79:C5:18:EF:25:6C:B0:7F:C7:FD:01:70:5C:EB` fingerprint

yubico-windows-code-2015.pem

SHA256 `1F:DA:33:2D:C3:DB:B7:DA:13:1B:BE:78:6E:2E:F9:2C:40:86:59:08:E5:C8:AA:1C:FC:F7:C6:5F:35:37:E3:7E` fingerprint

yubico-windows-code-2014.pem

SHA256 `DB:75:AF:B8:AF:DF:5C:DC:F9:70:1E:0E:FA:4C:44:97:ED:BE:0D:95:DB:8D:12:82:77:23:C6:6B:69:FE:3E:8B` fingerprint

Mac Software Signing

Our Mac executables are signed with a Yubico code signing certificate, issued by Apple.

yubico-mac-code.pem

SHA256 `11:52:AC:C2:27:7D:0E:76:59:D2:CC:DF:3A:BF:2D:ED:11:CF:F3:0D:67:C9:B5:B7:69:9B:CF:26:6F:4C:95:CE` fingerprint

Our Mac installers are signed with a Yubico code signing certificate, issued by Apple.

yubico-mac-code-installer.pem

SHA256 `A1:56:A5:D0:17:EB:D4:4D:4E:95:DE:06:A4:ED:BE:9F:3A:9C:23:9A:DE:13:66:9D:99:09:87:15:EA:B4:F3:38` fingerprint

Earlier Mac software may be signed with one of the following certificates:

yubico-mac-code-2017.pem

SHA256 `3C:3F:C5:78:DE:63:8A:96:A3:73:61:BD:3F:9C:39:55:DA:69:08:CD:C9:AF:57:8D:41:02:74:95:98:B8:98:83` fingerprint

yubico-mac-code-installer-2017.pem

SHA256 `CE:0A:F3:41:0B:9F:60:5E:D0:D4:7E:1E:D4:16:3C:0A:52:55:04:24:24:16:7A:0A:C8:3C:94:62:24:90:B9:CF` fingerprint

yubico-mac-code-2012.pem

SHA256 `F4:EC:6D:AF:9A:E6:AD:49:F6:D3:99:9A:D8:92:8E:A1:D3:A9:45:94:15:90:BC:33:BA:9D:8E:35:59:02:3C:BD` fingerprint