Yubico OID Reference Guide

Yubico

Sep 05, 2023

CONTENTS

CHAPTER

ONE

YUBICO OBJECT ID (OID) ARC

The arc from Yubico's OID is described in this guide. Object IDentifiers (OIDs) are a standardized method for naming objects, concepts, or persistent nameable things. The arc defines the subtree from Yubico's OID. Each node (the number between each dot) in the OID, identifies the controlling authority for that node.

Yubico's private enterprise OID is: 1.3.6.1.4.1.41482

Where -

`1.3.6.1.4.1` - identifies the authorities: `iso.identified-organization.dod.internet.private.enterprise`

`41482` - identifies Yubico

The Yubico OID including the arc, has the format: `1.3.6.1.4.1.41482.xx.xx`.

Where

`xx.xx` - are numbers that assigns a Yubico product type and attributes that are relevant to the product type. This can include physical type, certificate extensions, class, or other attribute. Also, depending upon the product type, the second node is not always used.

CHAPTER

TWO

OID PRODUCT ARC

2.1 Base Prefix

The values in the table are added to the Yubico OID to identify the Yubico product type.

`1.3.6.1.4.1.41482`

For the Form Factor OID, it matches the values for form factors listed in the Configuration Reference.

2.2 Yubico OID Allocation Arc Values

Within that arc, Yubico has a number of allocations. For each Sub-tree identified, additional OIDs are included to provide relevant details.

For attribute subtree values of the products, see their respective chapters.

Number	Description
1	U2F Device Type Sub-tree
2	U2F Device Identifier
3	PIV attestation Sub-tree
4	YubiCrypt attestation Sub-tree
5	OpenPGP attestation
6	Yk Quorum attestation Sub-tree
10	LDAP Classes
11	LDAP Attributes
12	FIPS
13	FIDO Attributes Sub-tree

2.3 Sample OID with Product Type

`1.3.6.1.4.1.41482.13` This represents an OID containted in an Attestation certificate for FIDO by Yubico. Within this certificate, each OID will include details specific to the FIDO credential and attestation certificate.

CHAPTER

THREE

YUBIHSM OIDS

When generating attestation certificates for keys, the YubiHSM will include OIDs listing specific information regarding the attested key.

3.1 Attestation

Asymmetric keys in the YubiHSM can be attested by another Asymmetric key. The attestation process creates a new x509 certificate for the attested key.

The device comes pre-loaded with an attestation key and certificate referenced by ID `0`. It is possible to use your own key and certificate for attestation, these then have to have the same ID and the key has to have the `sign-attestation-certificate` Capability set.

Details:

- Public key is copied from the attested key
- Serial is a random 16 byte integer
- Issuer is the subject of the attesting certificate
- Dates is copied from the attesting certificate
- Subject is the string "YubiHSM Attestation id 0x" with the attested ID appended
- If the attesting key is RSA the signature is SHA256-PKCS#1v1.5
- If the attesting key is EC the signature is ECDSA-SHA256

3.2 Certificate Extensions

Some certificate extensions are added in the generated certificate and the pre-loaded certificate:

OID	Description	Data Type
1.3.6.1.4.1.41482.4.1	Firmware version	Octet String
1.3.6.1.4.1.41482.4.2	Serial number	Integer
1.3.6.1.4.1.41482.4.3	Origin	Bit String
1.3.6.1.4.1.41482.4.4	Domains	Bit String
1.3.6.1.4.1.41482.4.5	Capabilties	Bit String
1.3.6.1.4.1.41482.4.6	Object ID	Integer
1.3.6.1.4.1.41482.4.9	Label	Utf8String

See:

- Domains
- Capabilities
- Object ID
- Label

3.2.1 Pre-loaded certificates

The pre-loaded certificate can be fetched as an opaque object with ID 0. This will in turn be signed by an intermediate CA which is signed by a Yubico root CA.

3.2.2 Intermediates

E45DA5F361B091B30D8F2C6FA040DB6FEF57918E.pem

3.3 Sample OID with Product Type

```
1.3.6.1.4.1.41482.13
```

CHAPTER

FOUR

FIDO PRODUCT OID ARC

FIDO protocols, including FIDO2/WebAuthn and U2F, support the generation of attestation certificates for generated credentials. These credentials will include OIDs listing details about the YubiKey itself. These OIDs are unique to Yubico FIDO Authentication devices, and may not be present on attestation certificates generated by non-Yubico hardware.

4.1 Base Prefix

The values in the table are added to the Yubico OID to identify the Yubico product type.

`1.3.6.1.4.1.41482`

4.2 FIDO2 and U2F Arc Values

When we change the physical appearance of devices or functional capablities, this list will be expanded.

4.2.1 FIDO Device Type

Number	Description
1	YubiKey U2F PlayStore devices (NXP-based) NB: We actually use the same cert for IFX based SKYs. JS 2015-08-24
2	YubiKey NEO (NXP-based)
3	YubiKey Plus (Infineon-based)
4	YubiKey Edge (Infineon-based)
5	YubiKey 4 USB (Infineon-based) [2015-11-03]
6	YubiKey NFC Preview (Infineon-based) [2018-04-12]
7	YubiKey 5 [2018-09-14]
8	YubiKey 5 Ci Lightning preview [2019-02-08]
9	YubiKey Bio

4.2.2 FIDO Attributes

Full prefix `1.3.6.1.4.1.41482.13`

Number	Description	Encoding
1	Firmware version	Octet string (3 bytes), Major, Minor, Patch, like: 040300 for 4.3.0
2	CSPN certification	Value marking which cert is relevant
3	Serial number	Serial number for enterprise attestation

For CSPN OID, this entry will only be present if the device has achived CSPN certification. For the Serial Number ODI, this entry will only be present on the Enterprise Attestation certificate, and will otherwise not be included.

4.3 Sample OID with U2F Type

Example for a YubiKey NEO:

version 1: `1.3.6.1.4.1.41482.1.2`

version 2: `1.3.6.1.4.1.41482.2: 1.3.6.1.4.1.41482.1.2`

Example for Yubikey 4 FIPS:

version 2: `1.3.6.1.4.1.41482.2: 1.3.6.1.4.1.41482.1.5 1.3.6.1.4.1.41482.12`

CHAPTER

FIVE

PIV ATTESTATION OID ARC

The attestation feature added to the PIV module in YubiKey 4.3 and 5. For actual commands to work with the attestation feature, see the yubico-piv-tool documentation.

The concept of attestation is used to show that a certain asymmetric key has been generated on device and not imported. Typically this would be used before creating a certificate.

5.1 Base Prefix

The values in the table are added to the Yubico OID to identify the Yubico product type.

`1.3.6.1.4.1.41482`

5.2 Implementation

Attestation is implemented by creating a X.509 certificate for the key that is to be attested, this is only done if the key has been generated on device. This certificate should be used for the purpose of verifying that the key was generated in device. Additional information included in the Attestation Certificate can be used to provide information about the device the attested key was generated on.

Some features of the generated certificate:

- Serial will be a random 16 byte integer
- Issuer will be the subject of the attesting certificate
- Dates will be copied from the attesting certificate
- Subject will be the string "YubiKey PIV Attestation " with the attested slot appended
- If the attesting key is RSA the signature will be SHA256-PKCS#1v1.5
- If the attesting key is EC the signature will be ECDSA-SHA256

The YubiKey comes with a pre-loaded attestation certificate signed by a Yubico PIV CA. This can be overwritten by loading a new key and certificate to slot f9. After the Yubico key is overwritten it can not be brought back. The attestation key and certificate will not be cleared out by a reset of the device.

Note: If you have a YubiKey Preview device, the attestation certificate will instead be signed by our Yubico PIV Preview CA

Note: The root cert for the Yubico PIV CA was updated on September 24, 2018. The prior PEM can be found here. YubiKey 4 Series manufactured prior to mid-2017 and some manufactured in 2018 were signed with Yubico's U2F Attestation CA.

For more information on support added to the current root certificate, see PIV Attestation Verification Fails with OpenSSL 1.1.0.

5.3 PIV OID Attestation Certificate Arc Values

The PIV Attestation certificates issued by Yubico have additional OIDs, used as certificate extensions.

Number	Description
1	Attestation data and signature
2	Attestation certificate
3	Firmware version
4	Applet version
5	Serial number Batch start
6	Serial number Batch end
7	Serial number (specific)
8	Usage policy
9	Form factor
10	FIPS
11	CSPN

5.4 Sample OID with PIV Type

Extensions in the generated certificate.

Certificate	Description
1.3.6.1.4.1.41482.3.3	Firmware version, encoded as 3 bytes, like: 040300 for 4.3.0
1.3.6.1.4.1.41482.3.7	Serial number of the YubiKey, encoded as an integer.
1.3.6.1.4.1.41482.3.8	Two bytes, the first encoding pin policy and the second touch policy - Pin policy: 01 - never, 02 - once per session, 03 - always - Touch policy: 01 - never, 02 - always, 03 - cached for 15s
1.3.6.1.4.1.41482.3.9	Formfactor, encoded as one byte - USB-A Keychain: 01 (81 for FIPS Devices) - USB-A Nano: 02 (82 for FIPS Devices) - USB-C Keychain: 03 (83 for FIPS Devices) - USB-C Nano: 04 (84 for FIPS Devices) - Lightning and USB-C: 05 (85 for FIPS Devices)
1.3.6.1.4.1.41482.3.10	FIPS Certified YubiKey
1.3.6.1.4.1.41482.3.11	CSPN Certified YubiKey

CHAPTER

SIX

OPENPGP ATTESTATION OID ARC

This document describes the OIDs present in the attestation certificates added to the OpenPGP module in YubiKey 5.2. For generating attestation certificates, you can use YubiKey Manager CLI (ykman) version 3.1.0 or higher.

The concept of attestation is to cryptographically certify that a certain asymmetric key has been generated on device, and not imported. This can be used to prove that no other copies of the asymmetric key exist. Yubico OIDs within the generated attestation certificate include contextual information about the device and key attested to.

6.1 Base Prefix

The values in the table are added to the Yubico OID to identify the Yubico product type.

`1.3.6.1.4.1.41482`

6.2 OpenPGP Arc Values

Number	Description	Encoding
1	Cardholder Name	UTF8 String
2	Whether generated on device	Integer (0 == imported, 1 == generated)
3	Firmware version	Octet string (3 bytes), Major, Minor, Patch, like: 040300 for 4.3.0
4	Fingerprint of the attested key (TAG C7/C8/C9)	Octet string, 20 bytes
5	Generation date of the key (TAG CE/CF/D0)	Octet string, 4 bytes
6	If the attested key is a SIG key, the current value of the Signature Counter	Integer
7	Serial number of the device	Integer
8	User Interaction Flag (UIF) if supported (TAG D6/D7/D8)	Octet string (1 byte), 00 - disabled, 01 - enabled, 02 - permanently enabled
9	Form factor	Octet string (1 byte) 00 - not specified, 01 - USB A Keychain, 02 - USB A Nano, 03 - USB C Keychain, 04 USB C Nano, 05 Lightning
10	FIPS	
11	CSPN	

6.3 Sample OID with OpenPGP Type

Full prefix `1.3.6.1.4.1.41482.5`

Extensions in the generated certificate:

OID	Type	Description
1.3.6.1.4.1.41482.5.1	UTF-8 String	Cardholder name
1.3.6.1.4.1.41482.5.2	Integer	Attested key's source - 0x00: imported (not permitted) - 0x01: generated on device
1.3.6.1.4.1.41482.5.3	Octet String (3)	YubiKey version number ex: 050303 = 5.3.3
1.3.6.1.4.1.41482.5.4	Octet String (20)	Attested key's fingerprint
1.3.6.1.4.1.41482.5.5	Octet String (4)	Attested key's generation date
1.3.6.1.4.1.41482.5.6	Integer	Attested key's signature counter (if applicable)
1.3.6.1.4.1.41482.5.7	Integer	YubiKey's serial number
1.3.6.1.4.1.41482.5.8	Octet String (1)	User Interaction Flag (UIF) - 0x00: touch disabled - 0x01: touch enabled - 0x02: touch permanent - 0x03: touch cached - 0x04: touch permanent, cached
1.3.6.1.4.1.41482.5.9	Octet String (1)	Form Factor - 0x00: Unspecified - 0x01: USB-A Keychain - 0x02: USB-A Nano - 0x03: USB-C Keychain - 0x04: USB-C Nano - 0x05: USB-C/Lightning Keychain
1.3.6.1.4.1.41482.5.10	Octet String (1)	FIPS Certified YubiKey
1.3.6.1.4.1.41482.5.11	Octet String (1)	CSPN Certified YubiKey

CHAPTER

SEVEN

LDAP EXTENSIONS OID ARC

7.1 Base Prefix

The values in the table are added to the Yubico OID to identify the Yubico product type.

`1.3.6.1.4.1.41482`

7.2 LDAP Arc Values

7.2.1 LDAP Class

Used for declaring Yubico specific class objects for schema extensions for LDAP servers

ID	Full Number	Name
1	1.3.6.1.4.1.41482.10.1	yubicoAttributes
2	1.3.6.1.4.1.41482.10.2	
3	1.3.6.1.4.1.41482.10.3	

7.2.2 LDAP Attributes

Used for declaring Yubico specific schema extensions for LDAP servers

ID	Full Number	Name	Description
1	1.3.6.1.4.1.41482.11.1	yubicoYubiOTP	TokenID:SEED:Counter:Metadata
2	1.3.6.1.4.1.41482.11.2	yubicoHOTP	TokenID:SEED:Counter:Metadata
3	1.3.6.1.4.1.41482.11.3	yubicoTOTP	TokenID:SEED:Counter:Metadata
4	1.3.6.1.4.1.41482.11.4	yubicoU2F	TokenID:KeyHandle:Counter:Metadata
5	1.3.6.1.4.1.41482.11.5	yubicoPublicKeys	TokenID:PublicKey:Metadata

7.3 Sample OID with LDAP Type

CHAPTER

EIGHT

FIPS CERTIFICATES OID ARC

The PIV Attestation certificates generated on the device will include OIDs with additional information about the YubiKey the certificate was generated on. For FIPS devices, there will also be an additional OID to indicate the YubiKey was FIPS certified. For all other devices, this OID entry will not be present.

8.1 Base Prefix

The values in the certificates are added to the Yubico OID to identify the Yubico product type.

`1.3.6.1.4.1.41482`

8.2 FIPS Arc Values

FIPS is marked with the OID `1.3.6.1.4.1.41482.12` and a value marking what FIPS certificate the device belongs to:

1: YubiKey Standard and YubiKey Nano Certificate #2267, validation date 10/14/2014 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/2267

2: YubiKey (4) FIPS Certificate #3204, validation date 6/21/2018 - 4/30/2019 (revoked but no keys programmed with this) https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3204

3: YubiKey (4) FIPS Certificate #3517, validation date 9/3/2019 https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3517

4: YubiKey 5 FIPS Certificate #3907 (Level 1), validation date (assuming this is the 4/22/2021 date but where is the other 8/19/2021 represented?) https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3907

5: YubiKey 5 FIPS Certificate #3914 (Level 2), validation date 05/03/2021 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3914

6: YubiHSM 2 Certificate #3916, validation date 05/03/2021 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3916

7: YubiKey 5 FIPS Certificate #3914 (Level 2) update, validation date 08/19/2021 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3914

8.3 Sample OID with LDAP Type

FIPS is marked with the OID `1.3.6.1.4.1.41482.12`

CHAPTER

NINE

COPYRIGHT

9.1 Copyright

9.1.1 Trademarks

9.2 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.

9.3 Contact Information

Yubico Inc.
5201 Great America Parkway
#122
Santa Clara, CA 95054
USA

https://www.yubico.com/support/contact/

More options for getting touch with us are available on the Contact page of Yubico's website.

9.4 Document Updated

2023-09-05 15:20:07 UTC