

# Key Lifecycle Management

---

**Version: 1.0**  
**Date: 9<sup>th</sup> September 2009**

### **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.

### **Trademarks**

Yubico and YubiKey are trademarks of Yubico AB.

### **Contact Information**

Yubico AB  
Kungsgatan 62  
111 22 Stockholm  
Sweden  
[info@yubico.com](mailto:info@yubico.com)

## Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Document history</b>                                | <b>4</b>  |
| <b>2</b> | <b>Definitions</b>                                     | <b>5</b>  |
| <b>3</b> | <b>YubiKey Manufacturing and Initial Configuration</b> | <b>7</b>  |
| 3.1      | Introduction   | 7         |
| 3.2      | Process overview                                       | 7         |
| 3.3      | YubiKey Manufacturing                                  | 8         |
| 3.4      | AES Key Lifecycle and flow                             | 8         |
| 3.5      | Key Generation   | 8         |
| 3.5.1    | Security of key generation                             | 8         |
| 3.5.2    | Key generation process                                 | 8         |
| 3.6      | Configuration Centres                                  | 9         |
| 3.6.1    | Physical Security of the configuration facility        | 9         |
| 3.6.2    | ICS computers used to configure YubiKeys               | 9         |
| 3.6.3    | Configuration process                                  | 9         |
| 3.7      | YubiKey Shipping office                                | 10        |
| 3.8      | Online Validation service                              | 11        |
| 3.8.1    | Online YubiKey Key Storage Module (YK-KSM)             | 11        |
| 3.8.2    | Online Yubico Validation Server                        | 12        |
| 3.9      | Re-configuration of YubiKeys by customers              | 12        |
| <b>4</b> | <b>References</b>                                      | <b>14</b> |

# 1 Document history

---

| Date       | Version | Author | Activity        |
|------------|---------|--------|-----------------|
| 2009-09-02 | 1.0     | KL     | Initial Release |
|            |         |        |                 |
|            |         |        |                 |
|            |         |        |                 |

## 2 Definitions

| Term                     | Definition   |
|--------------------------|--|
| AES                      | Advanced Encryption Standard. A NIST approved symmetric encryption algorithm. The Algorithm is considered very secure and used by military and financial institutions around the world.  |
| AES Key or Secret key    | Yubico uses Secret Keys in its generation of an OTP and in the process validating the OTP.<br>A secret key (aka symmetric key) means that the same key is used for encryption and decryption. Also see Key below.  |
| Configuration            | Refers to the configuration (burning) of devices. See ICS  |
| ICS                      | Initial Configuration System is the system that programs keys and identifying meta data into the YubiKeys at the time of manufacturing.  |
| Key or Encryption Key    | A Key is a parameter used as one input to a cryptographic algorithm for encryption, decryption, hashing etc. The key determines the functional output of a cryptographic algorithm. Simplified, with the Key the output from the algorithm is "readable" but without the correct key, the output from algorithm is not correct and unusable. |
| Key lifecycle            | The full lifecycle of an encryption key from creation to deletion  |
| Key Creation/ Generation | The process of generating, local storing and secure transferring of the encryption key that will be programmed into the YubiKey device.  |
| KGC                      | Key Generation Computer, generating the secret AES keys  |
| Key Record               | The information in the file or database that holds an individual key and associated meta information   |
| OTP                      | One Time Password. Use of OTP makes it difficult for attackers to gain unauthorized access to protected resources/services.  |
| OTP validation           | General term for the process of validating the correctness of the submitted OTP. The Validation process generates a Yes/No reply to the contacting service.  |
| PublicID / YubiKey ID    | The 0-16 character string programmed into a YubiKey which precedes the OTP when the button is pressed on a YubiKey. Normally 12 char.  |
| Programming              | Programming of keys. This is the process of storing certain information like the PublicID, the SecretID, the AES encryption key etc. into a YubiKey device. This is one of the steps in manufacturing of YubiKey devices executed after a YubiKey is assembled.  |
| SecretID / InternalID    | The 6 byte SecretID is a part of the 16 byte OTP token. This is always encrypted when the OTP is emitted by the YubiKey and transferred over the network.  |
| USB                      | Universal Serial Bus – The type of connector used by YubiKey   |

| Term                                     | Definition  |
|--|---|
| YubiKey                                  | Yubico's authentication device for connection to a USB port   |
| YubiKey Factory                          | Manufacturing Site that manufactures the YubiKeys   |
| YK-KSM                                   | Yubico Key Storage Module – A secure service storing the AES keys for servicing the online service.   |
| YK-Val<br>Validation<br>Server / Service | General term for Yubico Open Source Validation modules or Yubico Online Validation Service. Some are packaged as ready to use servers or services while other modules are to be integrated in a third party module or services to be YubiKey enabled. |

### 3 YubiKey Manufacturing and Initial Configuration

#### 3.1 Introduction

Blank YubiKeys are manufactured in bulk at a Yubico selected manufacturing unit and after testing shipped back to a Yubico warehouse for temporary storage. Blank YubiKeys then shipped in batches to a Configuration Centre where they are tested and configured (programmed) with a unique AES key and other device related meta information including identification data as part of the configuration process. After configuration and final testing the YubiKeys are packaged and shipped to one of the Yubico Shipment offices (currently located in Europe and USA).

#### 3.2 Process overview

The full configuration process begins with generating the secret AES keys to be programmed into the YubiKeys. The AES keys and other configuration meta data are generated by a dedicated Key Generation Computer (KGC) at a secure Yubico facility and then securely transferred in encrypted form after generation to both the Yubico Key Storage Module (KSM) at the Server Hosting Facility and to the selected Configuration centres (for the batch of YubiKeys to be configured).

Each Configuration centre has a dedicated computer known as the Yubico Initial Configuration System (ICS) which receives the initial configuration information for the batch of YubiKeys and configures the device information including the corresponding AES keys into the YubiKey devices. After testing, each YubiKey is labelled with a serial number for identification and packaged and shipped out to a Yubico Shipping Office.

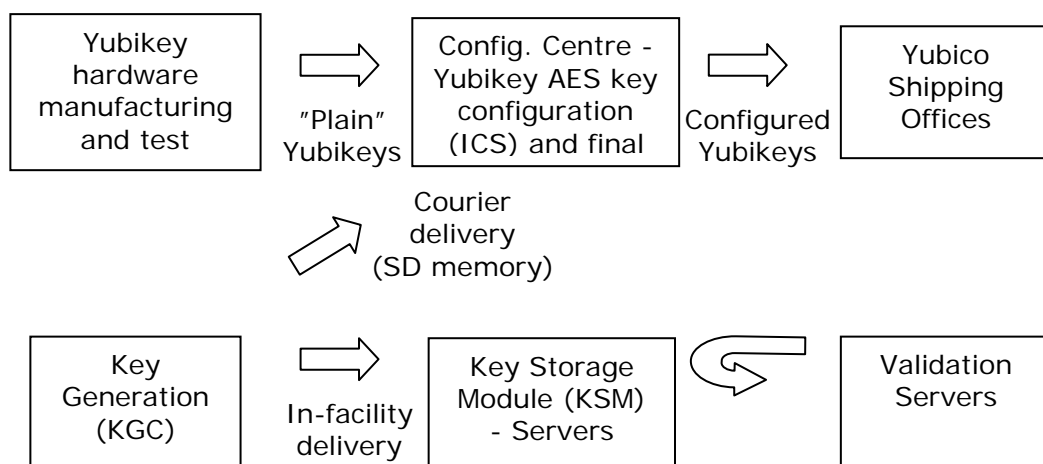


Figure 1- Flowchart of the process

The above chart briefly summarizes the manufacturing and configuration process. The detailed processes are described in the sections below.

Also at the end of the document we will cover reconfiguration of keys by the customer that can be performed at any time after manufacturing - using the Yubico Personalization tool.

### 3.3 YubiKey Manufacturing

Blank YubiKeys are manufactured in bulk at a Yubico selected manufacturing facility and after testing shipped back to a Yubico warehouse for temporary storage.

YubiKeys are manufactured in trays. Each tray holds  $4 \times 5 = 20$  devices per tray. These trays follow the units from the plastic moulding to initial testing by a testing computer and connected test rig.

All devices in a tray are tested. After testing the YubiKeys are separated from the tray and packaged for shipping to a Yubico warehouse.

### 3.4 AES Key Lifecycle and flow

The following services/entities are involved (sequentially) in key generation, initial configuration, distribution and operational stages of YubiKey AES-key lifecycle:

1. Yubico Secure facility Generating AES key records
2. YubiKey Configuration Centres
3. Yubico Shipping Offices (no access to AES keys)
4. Online YubiKey Key Storage Module (YK-KSM)
5. Online Yubico Validation Server (YK-Val)

The functionality of each is described in detail below:

### 3.5 Key Generation

The Key generation is performed in a monitored and highly secure facility and operated by specially authorized Yubico personnel.

#### 3.5.1 Security of key generation

The Key Generation facility and equipment are sensitive to both theft and manipulation. The key generation equipment is therefore locked in a safe when not in use. The Key Generation Computer KGC has full-disk encryption and requires a password comprising a YubiKey with a strong static password plus an additional user password.

The KGC computer system is for security reasons never connected to any network. Once the practical end-of-life of the computer is reached the main key to the disk-encryption is deleted and therefore the drive will be rendered irrecoverable. In addition the hard disk will be physically incinerated.

#### 3.5.2 Key generation process

The KGC generates AES keys and associated initialization information such as SecretID and YubiKeyID. The KGC uses a high quality pseudo random value generator module when generating the AES Key, Secret ID and lock code for each YubiKey that later on in the process will be configured into each YubiKey.

When a new batch of YubiKeys shall be configured the KGC generates the AES keys and corresponding meta data to be programmed and stores the information for each YubiKey in a key record (file), one for each YubiKey.

Public Private Key technology (OpenPGP) is used to protect the key record files for the whole batch. The KGC uses a public key unique for each Configuration centre's Initial Configuration System (ICS) computer when encrypting key records files. When desired keys records have been generated all the key record files for the batch are zipped into one zip file. The zip file is finally stored on a SD card. The SD card with the zip file is sent to the Configuration site.

If the AES keys are needed to be uploaded to the online YK-KSM server (normal case), the application programs re-encrypts the individual records with the public key of each YK-KSM. The OpenPGP encrypted file containing the records is sent to the YK-KSM servers using public-key protected OpenSSH. Each YK-KSM decrypts and verifies the signature of the data and performs a final check to verify that Public IDs are unique. If a duplicate is found the YK-KSM will write an error log and discard the record.

### 3.6 Configuration Centres

As a device manufacturing factory typically cannot handle sensitive information in a structured way, an intermediate configuration facility is used to perform the actual Yubikey configuration and apply appropriate visual marking on the configured YubiKeys.

#### 3.6.1 Physical Security of the configuration facility

The configuration facility and the configuration equipment are sensitive to both theft and manipulation. The configuration process is therefore handled by specially authorized and trained personnel. The configuration equipment, holding the key SD card and private key to unlock them, is physically stored in a safe when not in use

#### 3.6.2 ICS computers used to configure YubiKeys

Each Configuration facility has a special purpose programming computer for initialization/programming of YubiKeys. This computer is called Initial Configuration System (ICS) and is used to program the AES key and corresponding metadata in each YubiKey. Each configuration computer being a part of the configuration equipment is pre-configured at the Yubico secure facility where also the unique private-public key pair for the ICS is generated. The computer facilitates full-disk encryption that is unlocked by a Yubikey in static mode plus a password. Each operator being trusted in using the configuration equipment has a private Yubikey that is stored in a physically different location.

#### 3.6.3 Configuration process

YubiKeys for the batch to be configured are shipped to the Configuration center from the Yubico warehouse.

Each Yubico Configuration facility is assigned with a unique YubiKey ID prefix. The programming ICS computer at each facility is configured to use

a YubiKey ID for each YubiKey in sequence starting from the already assigned YubiKey ID prefix.

The ICS computer is connected to the rig equipment that programs each YubiKeys with a sequential YubiKey ID, random SecretID and unique AES Key.

For each batch the SD card containing the AES keys and meta data for the batch is inserted into the ICS and after the associated Yubikey (separately shipped) has been used to unlock the zip file, the key record files are extracted into a dedicated programming directory. Each key record file is securely deleted after successful programming and testing of a YubiKey. During the configuration of the batch a log file containing each operation successful as well as unsuccessful are written to the disk and the SD card.

The steps involved in configuration of the YubiKeys at the Configuration facility are as follows:

1. Key records moved from the SD card to a dedicated key directory for YubiKey key records on the ICS computer
2. The zip file on the SD card (with the key record files) is securely deleted.
3. 8-16 non programmed YubiKeys are inserted into the programming rig of the ICS computer
4. The ICS computer then decrypts each encrypted file record and prepares to configure each of the 8-16 YubiKeys with sequential YubiKey IDs and corresponding AES Key and SecretID.
5. Operator presses the start button
6. Configuration and testing of each YubiKey takes place
7. After successful configuration operation, the encrypted key records for each programmed YubiKey is securely deleted from the key directory and a log written to a log file on the computer and on the SD card
8. If the operation was unsuccessful the key record is still deleted but an error is recorded in the log file on the computer and in the SD card
9. The ISC computer then generates the bar codes with a serial number for the YubiKey which are the linked to the sequential YubiKey IDs
10. Each YubiKey is then added in sequence into a plastic packaging/sleeve and adding a sticker for the corresponding serial number/bar code
11. YubiKeys are then added into a bag in batches of 10. Then 10 bags (with 10 YubiKeys) are placed in a small box. 10 small boxes fit in a larger box. The large box then holds 1000 YubiKeys.
12. These large boxes are then transported to the Yubico Shipping office together with the SD card used in the process for this batch so that the encrypted log files can be reviewed by Yubico authorized personnel.

Optionally, for an extra fee, a customer identification text or logo can be printed on the devices.

### 3.7 YubiKey Shipping office

The Yubico shipping offices are currently located in the UK and California, USA. The centers receive shipments of configured batches of YubiKeys from the Configuration centers.

When orders come in from the Yubico Web store, Partners or the Yubico Sales team, orders are entered or transferred into a CRM system and shipping information is generated, listing shipping information including the serial numbers of the YubiKey shipped to each Partner or Customer.

The Shipping Offices do not have access to AES keys nor have they credentials to upload keys to the YK-KSM.

### 3.8 Online Validation service

For security reasons the Online Validation Service is split in two distinct systems, one Validation Service (servicing Validation requests) and multiple YubiKey Key Storage Module (YK-KSM or just KSM) where all the AES keys are securely stored.

A brief explanation of how the system works in action is as follows:

1. The Validation Server gets a OTP validation request, either over HTTP or HTTPS
2. If the request is signed, the validation server checks the signature and reports back an error on failures
3. It connects through to the YK-KSMs to have the OTP decrypted
4. One KSM responds with the decrypted OTP (over a secure link)
5. The Validation Service can then validate the OTP by comparing the decrypted data with the counter values stored in a local database
6. The Validation service sends a signed response back to the requester

The Yubico Validation Service and YK-KSM have been designed for scalability, and benchmarking shows that it can handle well above a thousand requests per second with a database consisting of 10 million records. The system currently is built around Apache, MySQL and PHP and supports multiple concurrent requests.

As a summary when it comes to where authentication data is stored. The YK-KSM stores the AES Keys and a copy of the YubiKey ID while the Yubico Online Validation Server will store the Meta Data including Identifiers but not the AES Key.

#### 3.8.1 Online YubiKey Key Storage Module (YK-KSM)

The online YubiKey Key Storage Module (YK-KSM) stores the AES keys of the YubiKeys shipped to the customers. The YK-KSM server runs on a secure server hosted at the server hosting facility. The YK-KSM server is completely secured physically. It is located behind an Internet Firewall and the YK-KSM server listens only to a single port and accepts connections only from selected IP addresses. The communication with Validation Server is TLS protected.

The YK-KSM server decrypts the uploaded records and stores the corresponding YubiKey ID, Internal ID, lock code and AES keys of every YubiKey in its database.

The YubiKey users send the OTP validation requests to the Yubico validation server. The validation server sends the encrypted OTP to YK-KSM server. YK-KSM server looks for the AES Key into its database by using the YubiKey ID prefix which is part of the OTP. Using the AES Key retrieved from the database, the YK-KSM server decrypts the OTP and sends back the decrypted OTP to the validation server.

### 3.8.2 Online Yubico Validation Server

The primary responsibility of the online Yubico Validation Server is to validate the OTP. Whenever the validation server receives an OTP validation request, it extracts the OTP part from the request and sends it to the YK-KSM server for decryption. If the YK-KSM server is able to decrypt the OTP (checks the internal ID and CRC for consistency), it sends "success" status response and the decrypted OTP back to the validation server, otherwise it sends only a failure status.

Depending on the response received from the YK-KSM server, the validation server validates the OTP, or sends error message back to the requesting process. If the response from the YK-KSM server is positive, the validation server checks the decrypted OTP parameters with the values stored in the database. If all the OTP values are correct, the validation server sends success status message, otherwise it sends a failure status message.

If no corresponding YubiKey record is already present in the database, the validation server inserts a new record for the YubiKey to its database and sends success response to the validation request. In this case the YKID and counters are also automatically created by this process.

## 3.9 Re-configuration of YubiKeys by customers

For high security environments, customers may select not to share the AES key information for their YubiKeys outside of their organization. Customers may also for other reasons want to be in control of all AES keys programmed into the Yubikey devices. Yubico therefore supports the use of a personalization tool to reconfigure the YubiKeys with new AES keys and meta data.

Please note that when reconfiguring YubiKeys the previous configuration is overwritten by the new configuration and the old configuration cannot be recovered once overwritten. For YubiKey 2.0 and later releases you can chose to change configuration slot 1 or slot 2. Slot 1 contains the configuration preset by the configuration center. Slot 2 is by default unused. They can both be configured individually (e.g. a reconfiguring of slot 1 will only affect the settings for slot 1 and leave the configuration in slot 2 intact).

For validation to work after reprogramming (when keys are not shared), the customer needs to setup their own Validating Server and YK-KSM and store the AES key(s) in the YK-KSM server database and the relevant meta data in the Validation Server database.

However, these new keys can, if the customer so chooses, also be uploaded back to the Yubico online service in case there is a need to also use the YubiKey to access connected online services.

The personalization tool can be used to:

- Change AES key
- Change the YubiKey ID (aka PublicID)
- Change SecretID (aka InternalID or PrivateID)
- Configure a YubiKey to generate static password instated of OTP
- Configure a security programming password to prevent malicious or accidental reconfiguration of YubiKey configuration.

The following process is recommended for reconfiguration of YubiKeys:

- Use the YubiKey Personalization tool (available for Windows, Mac OS X and Linux)  
(<http://www.yubico.com/developers/personalization/> )
- Set up and configure the required parameters
- Configuration (Programming) of keys
- Uploading of AES key records to the online Yubico server using a secure interface provided by Yubico. Please refer to <http://www.yubico.com/developers/aeskeys/> for more details.
- If there were duplicate IDs (i.e. IDs already existing in the database) during the upload, no record is uploaded. An error message will be displayed listing one or more duplicates. Duplicate records must be deleted before upload can be attempted again.
- Testing – once the upload is successful you can test the uploaded YubiKey information by trying one of the uploaded keys with the online Yubico validating server [at http://www.yubico.com/one](http://www.yubico.com/one)

## 4 References

---

1. YK-KSM and YK-VAL, Yubico,  
<http://yubico.com/developers/srv/>
2. Yubico Personalization Software, Yubico,  
<http://yubico.com/developers/personalization/>