



YubiCloud OTP Validation Service Guide

Copyright

© 2016 Yubico Inc. All rights reserved.

Trademarks

Yubico and YubiKey are registered trademarks of Yubico Inc. All other trademarks are the property of their respective owners.

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.

Contact Information

Yubico Inc

420 Florence Street, Suite 200

Palo Alto, CA 94301

USA

yubi.co/contact

Document Release Date

July 8, 2016

Contents

Introduction	4
YubiCloud OTP Validation Service	4
Getting Additional Help	5
Understanding the YubiCloud OTP Validation Service	6
Redundant Services	6
Validation Process	7
Components	8
Validation API Software	9
Synchronization Between Servers	9
Secure Production Process	10
Provisioning AEADs	11
Uploading the AES Key	12
Generating an API Key	13
Hosting Environment for the YubiCloud OTP Validation Service	14
SAS 70/SSAE 16 Standard	14
RAID Storage	14
Redundant Internet Connections	15
Backup and Restore Process	15
Uptime Specification	15
Security	15
Patch Management	15
Archiving Access Logs	16
Service Availability Monitoring	16
Uninterrupted Power Supply	16
HVAC Support	16

Introduction

Yubico changes the game for strong authentication, providing superior security with unmatched ease-of-use. Our core invention, the YubiKey, is a small USB and NFC device supporting multiple authentication and cryptographic protocols. With a simple touch, it protects access to computers, networks, and online services for the world's largest organizations.

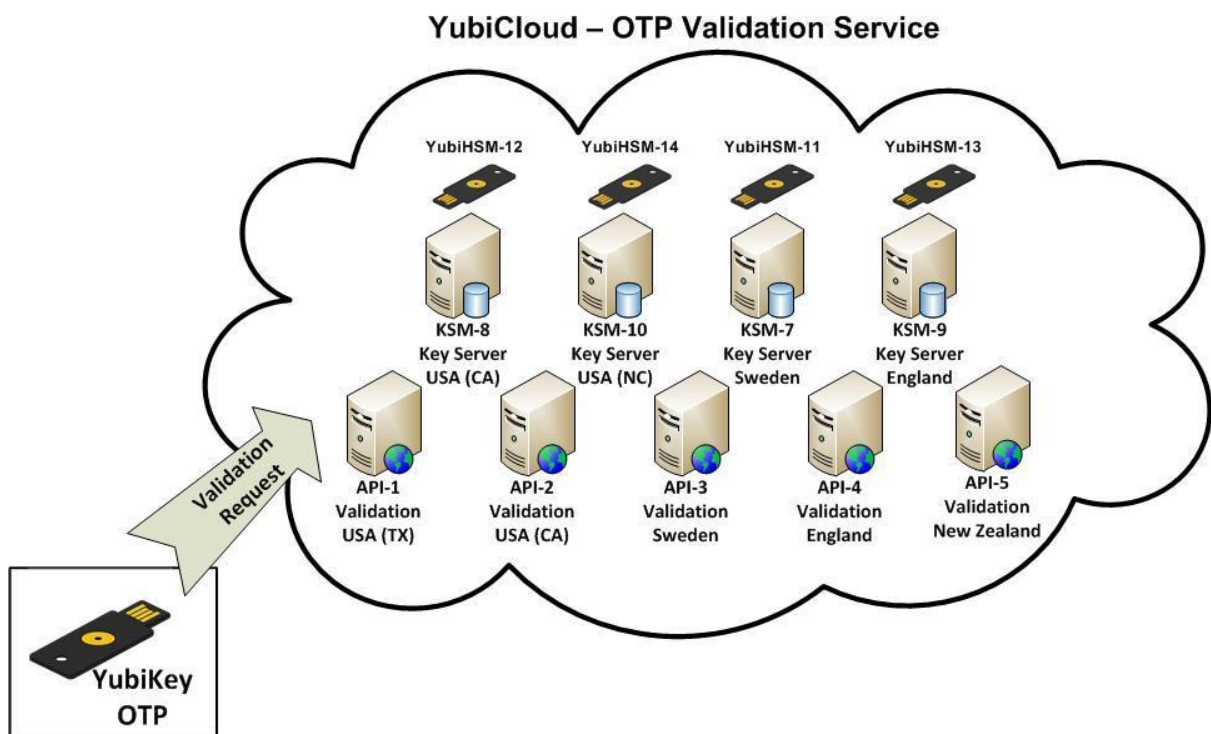
Our innovative keys offer strong authentication via Yubico one-time passwords (OTP), FIDO Universal 2nd Factor (U2F), and smart card (PIV, OpenPGP, OATH) — all with a simple tap or touch of a button. YubiKeys protect access for everyone from individual home users to the world's largest organizations.

YubiCloud OTP Validation Service

This document describes the YubiCloud OTP Validation Service that provides cloud-based Yubico OTP validation to customers and partners in a convenient, secure, and reliable manner. Both the service and the supporting services for importing YubiKeys, building a production topology, and creating a hosting environment for the service are described here.

The YubiCloud OTP Validation Service is an online YubiKey validation service with redundant servers located in secure data centers at strategic locations around the world.

This document focuses on the YubiCloud validation service and describes how the demanding requirements are fulfilled by the 24x7 operation of the Yubico online validation service. All geographical and server number references are subject to change without notice.



This document describes the following topics:

- [Understanding the YubiCloud Validation Service](#)
- [Hosting Environment for the YubiCloud Validation Service](#)

Getting Additional Help

For more information, and to get help with your YubiKeys, see:

- [Support home page](#)
- [Documentation and FAQs](#)
- [Start a Support ticket](#)

Understanding the YubiCloud OTP Validation Service

The YubiCloud OTP Validation Service was launched March 2010 and the service has had almost 100% availability since the launch. YubiKeys are shipped ready to use with the YubiCloud validation service (no programming of the keys is required by the customer).

In this Chapter

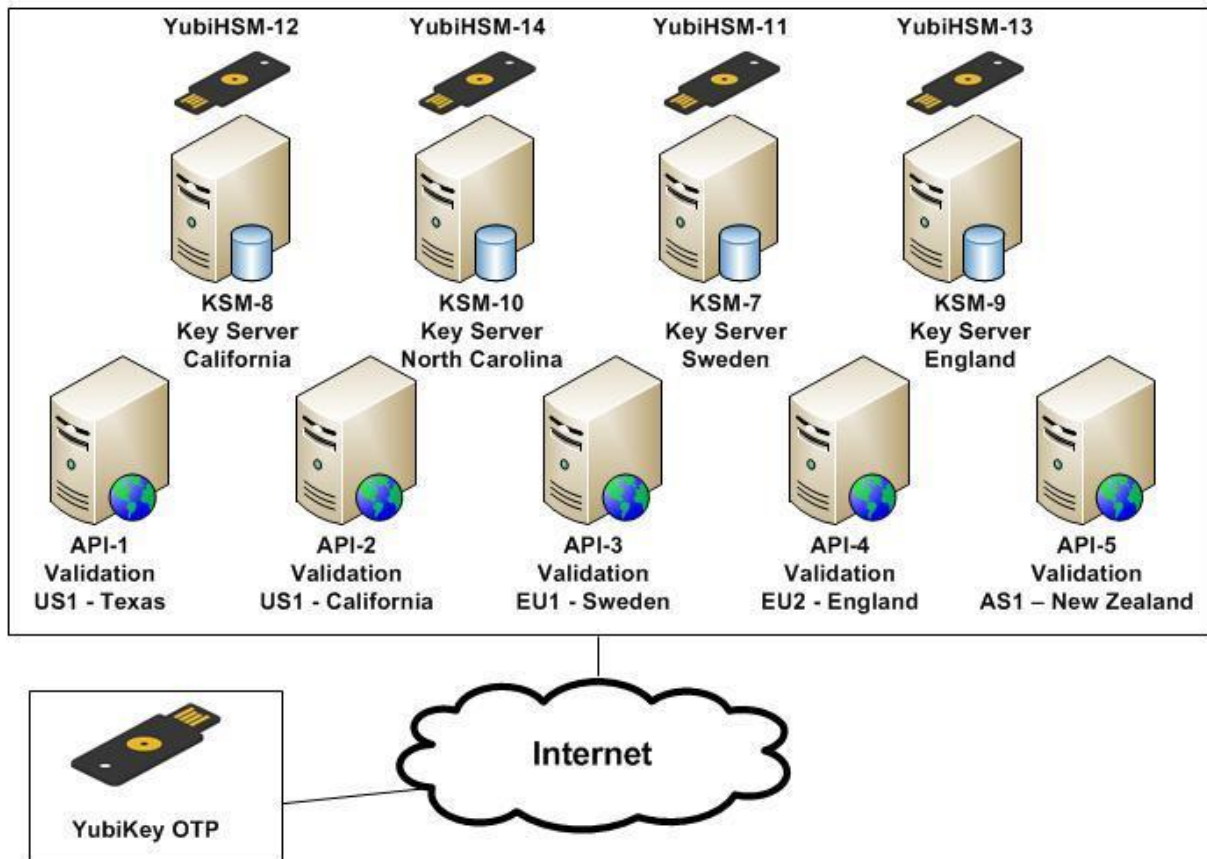
- [Redundant Services](#)
- [Validation Process](#)
- [Components](#)
- [Validation API Software](#)
- [Secure Production Process](#)
- [Provisioning AEADs](#)
- [Uploading the AES Key](#)
- [Generating an API Key](#)

Redundant Services

The YubiCloud OTP Validation Service is a cloud-based Yubico OTP validation service used to validate one-time passwords. The YubiCloud validation service makes it easy to add first class two-factor authentication to your login environment, which can be a web service or OS login. Our robust validation servers are arranged in a distributed failover configuration at five different locations around the world, all synchronized with each other. This ensures that there is no single point of failure and that responses are serviced in a timely manner, independent of the geographical origin of requests.

Each Key Storage Module (KSM) back-end server is equipped with a YubiHSM Hardware Security Module(s) to make sure that all secret keys are fully protected and stored encrypted at all times. There is no access to AES secrets (even for administrators of the back-end KSM servers).

YubiCloud – OTP Validation Service



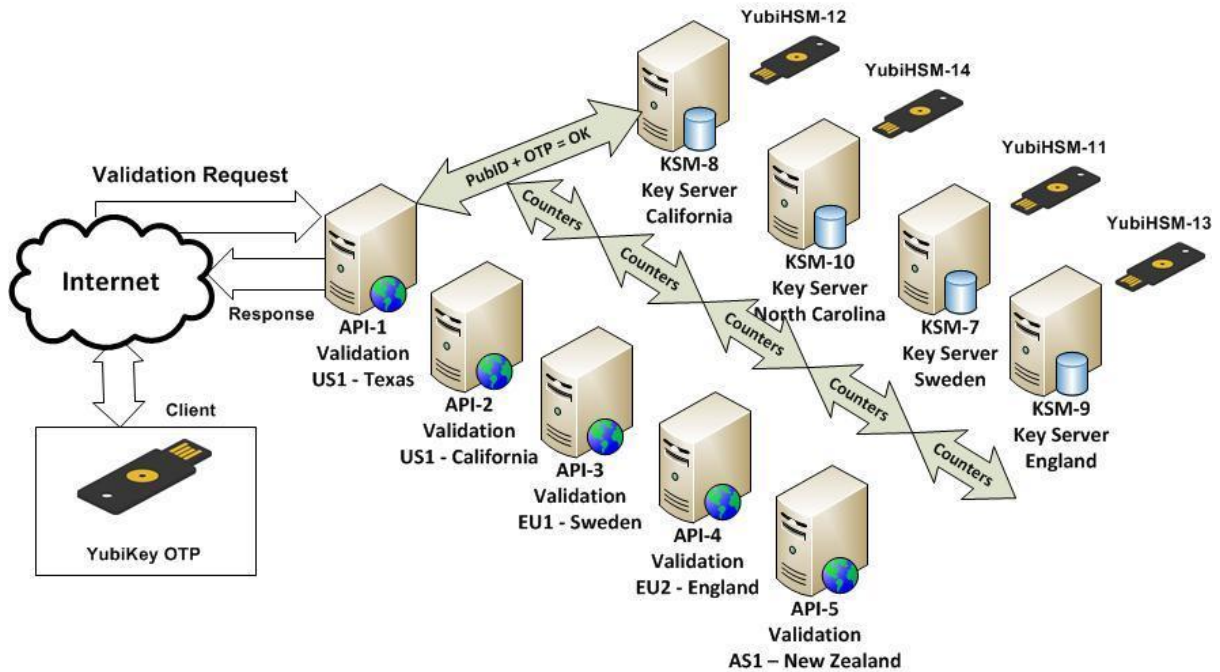
Validation Process

The validation process works by having the client send parallel requests to all servers supporting the YubiCloud validation service. A parallel approach has two advantages:

1. Latency is reduced to a minimum since the client does not need to wait for the response that takes the longest to return
2. Availability is improved because even if several validation servers are unreachable from the client's network, validation works correctly because:
 - Each validation server sends parallel requests to all KSMs to decrypt the OTP and uses the quickest response, reducing latency while maximizing availability.
 - Each validation server sends the OTP to all the other API servers to make sure that all validation servers have the same counter information for each YubiKey.
 - Synchronization requests are queued in case of temporary network outages.

For more technical details about the validation server software and algorithms, see the [yubikey-val software documentation](#).

YubiCloud – OTP Validation Service

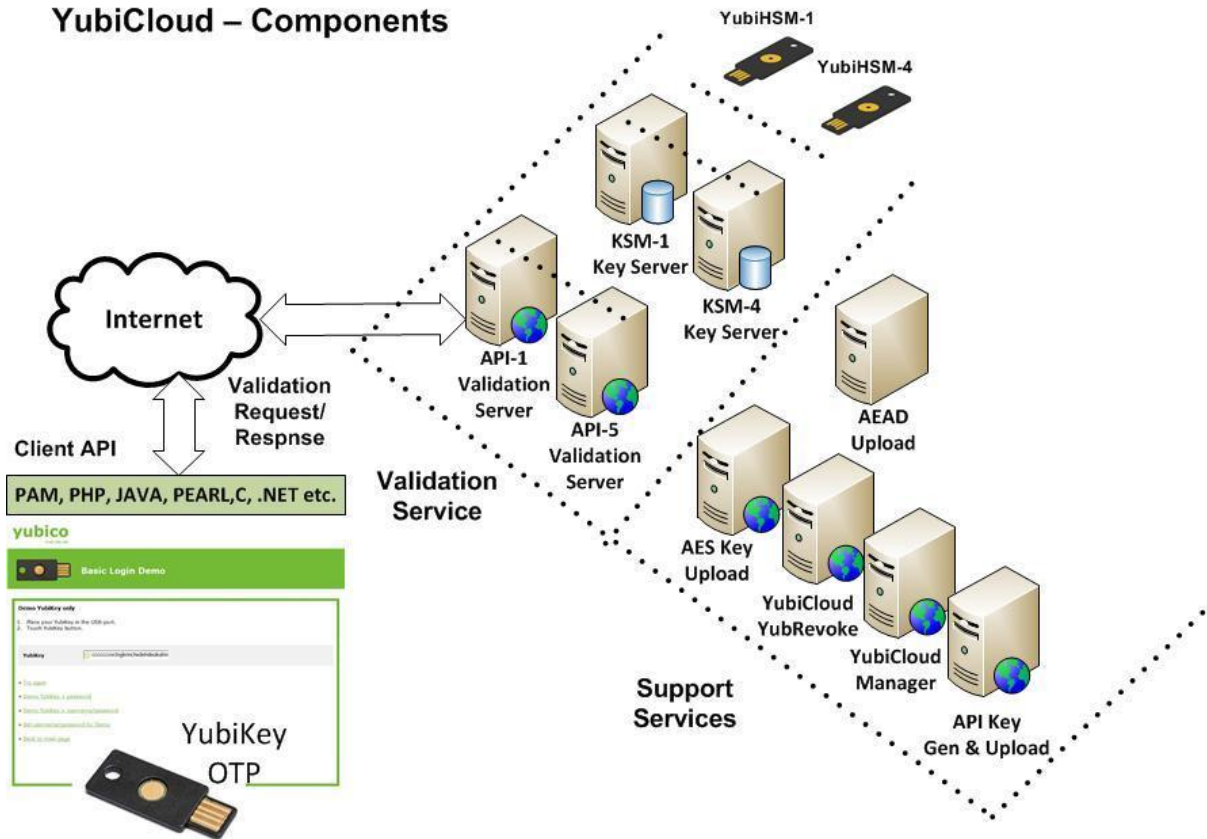


Components

The YubiCloud validation service consists of the following core components:

- Validation services:
 - Validation servers
 - Key Storage Modules (KSMs)
 - YubiHSMs
- Supporting services:
 - Key upload
 - YubiKey revocation service
 - API key generation

YubiCloud – Components



Validation API Software

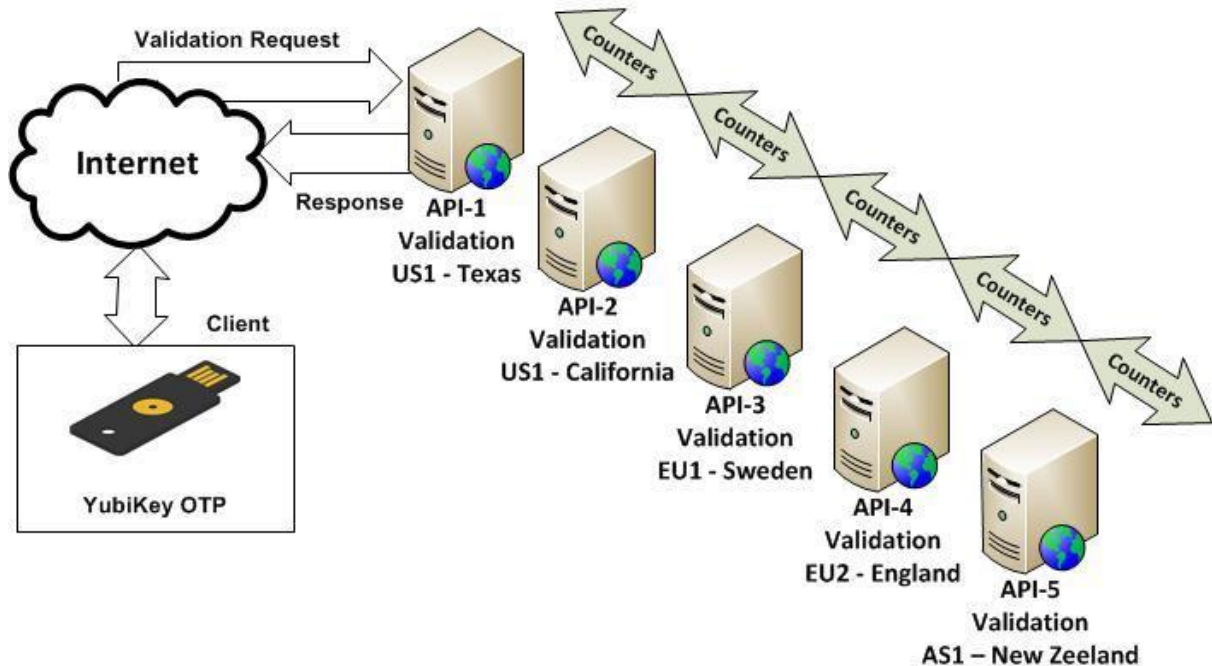
To add YubiKey two-factor authentication to your application or web service through the YubiCloud validation service, you can use just one of the client software applications and have your connection to the YubiCloud validation service operating in a few hours or less. See the [Yubico Developers website](#) for a list of current client software.

Synchronization Between Servers

The YubiCloud validation service synchronizes the counters between servers. The following image shows a simplified diagram for conceptual understanding of the synchronization process.

The details of the synchronization process are available in the [yubikey-val documentation](#).

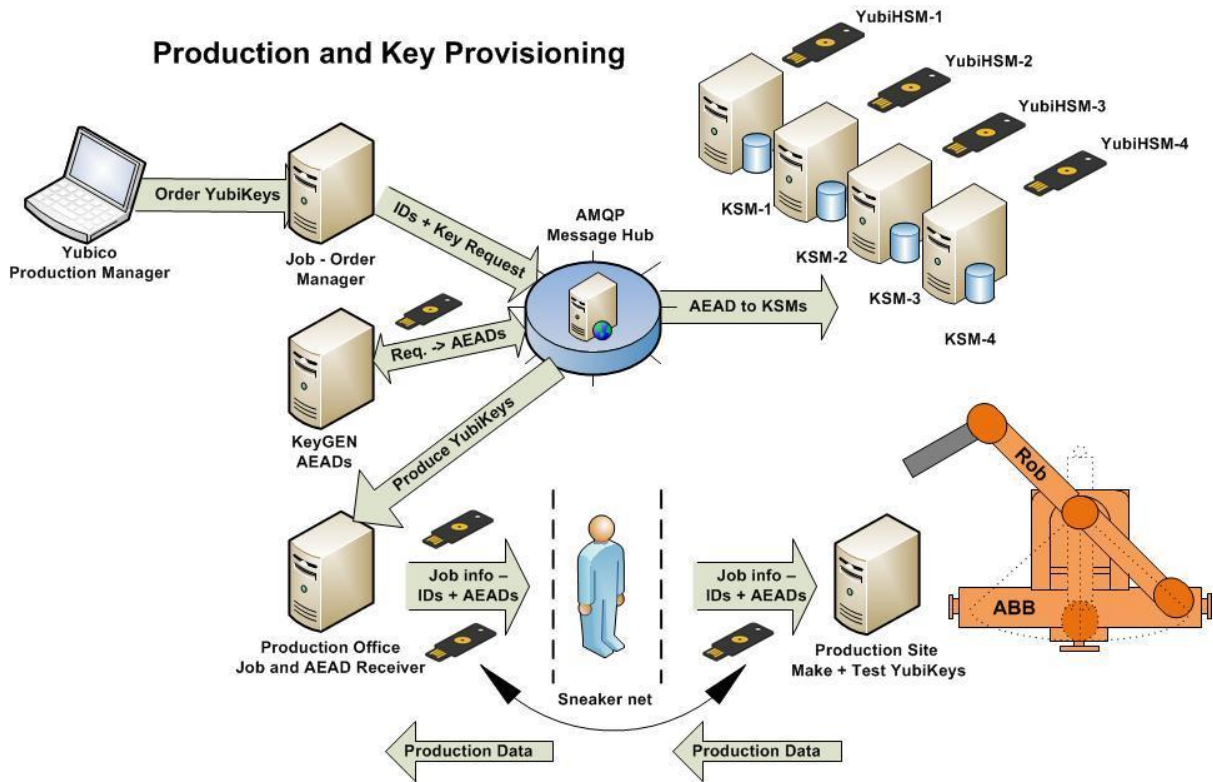
YubiCloud – Sync of OTP Counters between Validation Servers



Secure Production Process

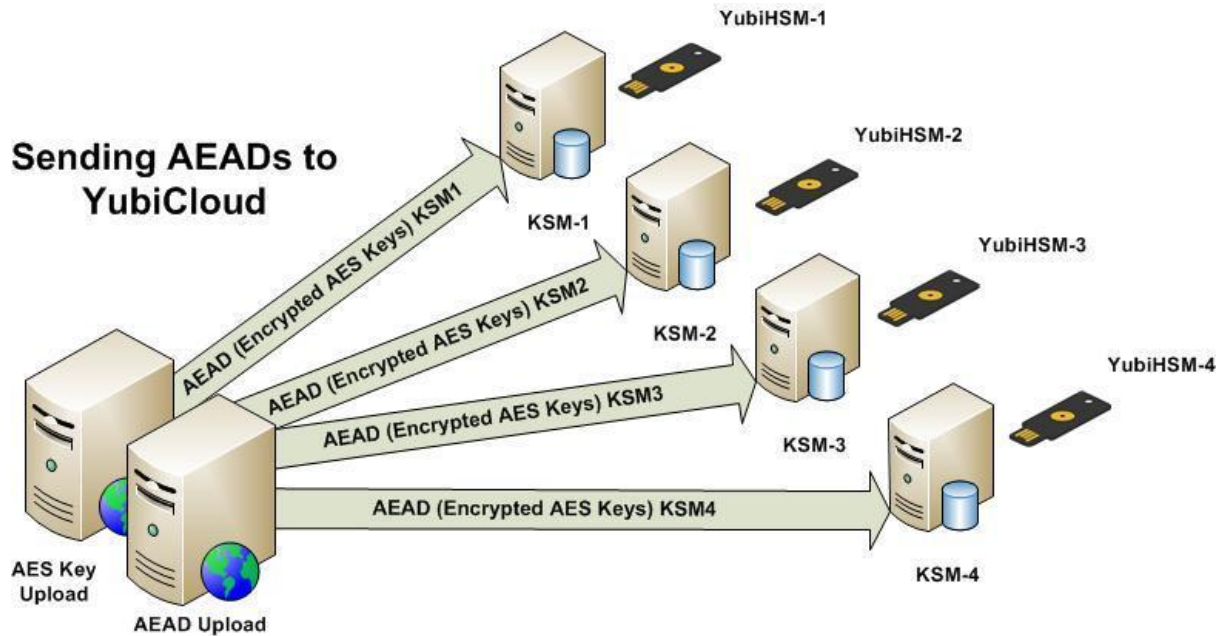
To provide a secure YubiCloud environment it is important that the production process is secure. The production process can be summarized as follows:

1. Data entry personnel enter the production orders based on logistical and manufacturing decisions.
2. An automated request is sent to a key generation (KeyGEN) computer, which includes a YubiHSM that is responsible for:
 - Generating new AES secrets for each YubiKey
 - Encrypting the secrets to a key available on the YubiHSM that is attached to each KSM
3. The KeyGEN YubiHSM encrypts the AES secret to the production facility, which is also equipped with a YubiHSM, and a logical escrow facility (not shown in the following diagram since it is not a physical machine) that is used manually when a new KSM is deployed.



Provisioning AEADs

Encrypted keys (AEADs), which are uploaded to the KSMs of the service, are provisioned using a message bus technology (AMQP) allowing for asymmetric upload. Asymmetric uploading is queuing messages so that the AEADs are provisioned separately to each KSM when the KSM is online. After they are provisioned, the AEADs are automatically deleted from the queue. Using this technology, the YubiCloud validation service is not dependent on having all servers available at the time of key provisioning.



Uploading the AES Key

Users are allowed to reprogram their Yubikeys and can upload the AES key (the secrets loaded on the YubiKey used for authentication) using our online web-based interface. An AES key begins with `vv`, and once uploaded to the [YubiCloud server](#), it cannot be removed or replaced.

Please enter information about your newly personalized YubiKey.

Please note: It takes 15 minutes for an uploaded identity to become valid on our validation servers. Please wait 15-20 minutes before testing an uploaded identity.

Your e-mail address:


Serial number:

YubiKey prefix:

Internal identity:


AES Key:

OTP from the YubiKey:



tice

Skriv båda orden:



stop spam. read books.

For more information about uploading the AES key, see the [Yubico website](#).

Generating an API Key

To be able to sign requests to the YubiCloud validation servers, and to be able to verify responses from the YubiCloud validation servers, you need to request an API identity and key. The identity is a decimal integer and the key is an HMAC-SHA1 secret generated by Yubico.

To get an API identity and key

1. Go to the [Yubico website](#).
2. Type your email address.
3. Authenticate using your YubiKey:
 - a. Insert your YubiKey into a USB port of your computer.
 - b. Place your cursor in the **YubiKey one-time password** field, and touch the YubiKey button.
 - c. Click **Get API Key**.

IMPORTANT: Users manage their own API keys. API keys are not managed by Yubico. If users lose their API keys, they just create new ones.

Hosting Environment for the YubiCloud OTP Validation Service

Servers forming the YubiCloud validation service are located in secure hosting facilities in Europe, the United States, and Asia.

The Yubico Key Storage Modules (KSMs) operate on dedicated servers called key servers. Each key server has a YubiHSM in a USB port, which stores the key server encryption keys and performs the actual OTP decryption. If the key servers are compromised, the AES keys are not exposed.

This chapter describes the server standards and configurations for the YubiCloud validation service hosting environment.

In this Chapter

- [SAS 70/SSAE 16 Standard](#)
- [RAID Storage](#)
- [Redundant Internet Connections](#)
- [Backup and Restore Process](#)
- [Uptime Specification](#)
- [Security](#)
- [Patch Management](#)
- [Archiving Access Logs](#)
- [Service Availability Monitoring](#)
- [Uninterrupted Power Supply](#)
- [HVAC Support](#)

SAS 70/SSAE 16 Standard

SAS 70 and its successor standard, SSAE 16, are audit standards that define the set of internal control objectives that are important to our customers and provide assurance on the design and operational effectiveness of those controls.

Although not all the facilities used for hosting the servers in the YubiCloud validation service have the above certifications, they have equivalent procedures in place.

RAID Storage

Servers are configured with RAID redundant storage for continuous uninterrupted service (in the event of disk failure).

Redundant Internet Connections

Servers are configured with 1 Gbps LAN adapters that are connected to the internet through a set of redundant switches and firewalls. The switches and firewalls are connected to a multiple gigabit connection with failover capabilities that provide speed and uninterrupted network access.

Backup and Restore Process

The Yubico validation service backup process is configured to take a complete backup of the entire database and application data to a remote server on at least a daily basis. Backups are encrypted when transferred and are kept for at least one year. The software used is rsnapshot.

Uptime Specification

The Yubico validation service is offered at no charge on a reasonable-effort basis. We make an effort to resolve issues quickly and are committed to offering the best service we can deliver. If you have special needs, please contact us to negotiate a committed uptime guarantee.

Security

The hosting facility has capabilities to protect the integrity of hosted data, and guards against service interruptions due to security issues.

The hosting facility provides complete physical, system, and operational security against different types of threats.

The security provides:

- Staff to provide monitoring against unauthorized entry 24x7
- Several CCTV security cameras monitoring the data center 24x7
- System installation monitored to use latest upgrades
- Firewalls to prevent unauthorized system access
- All cabinets and cages locked, ensuring maximum security
- No visitor access to server rooms
- No onsite maintenance work on systems

Patch Management

We perform scheduled and timely security patching of the operating system and all standard software modules used by the YubiCloud OTP Validation Service. Since the nature of the YubiCloud validation service is that there is no single point of failure, server maintenance and upgrades are performed immediately when OS vendor upgrades are available. This policy can result in a few minutes downtime of a particular server but does not lead to any interruption of the YubiCloud validation service.

Archiving Access Logs

The YubiCloud validation service provides secure archiving of the system and access logs to allow quick diagnostics of any failure.

Service Availability Monitoring

The Yubico Support team is continuously monitoring the availability and performance of the YubiCloud OTP Validation Service and Yubico KSM using Nagios/Icinga monitoring software and through the online monitoring service, Pingdom. Customers can follow our incident reporting and uptime graphs on the [Yubico website](#).

In the event of application (software) failure, the monitoring service notifies the team immediately through email and SMS for prompt action.

Uninterrupted Power Supply

Each hosting facility provides uninterrupted power supply along with backup power units to the YubiCloud OTP Validation Server, KSM server, and other network and system infrastructure.

The hosting facility is fitted with a conditioned uninterrupted power supply and diesel-powered generator equipped with an automatic transfer switch between power sources.

HVAC Support

The facility provides YubiCloud servers with HVAC that has redundancy so that the required temperature and environment for YubiCloud OTP Validation Service are maintained at all times.

The HVAC system for the YubiCloud validation service includes:

- Redundant chillers and multiple air conditioning units pumping cold air into the raised floor of the data center
- Self-contained VAC units that provide ample cooling power
- VAC units carefully monitored daily by onsite personnel
- Humidity controller ensures optimal operation