

YubiCloud Validation Service

Version 1.0

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 37, 8th floor
111 56 Stockholm
Sweden

info@yubico.com

Content

1	Document Information	4
1.1	Purpose	4
1.2	Audience	4
1.3	References	4
1.4	Document History	4
1.5	Definitions.....	4
2	Introduction.....	5
3	The YubiCloud	6
3.1	Redundant Services	6
3.2	Validation Process.....	7
3.3	Components	8
3.4	Validation API software.....	8
3.5	Sync between servers.....	8
3.6	Production	9
3.7	Provisioning AEADs.....	9
3.8	AES Key Upload.....	10
3.9	API Key	10
3.9.1	Management of API Keys	10
3.10	YubiRevoke	10
4	Hosting Environment for YubiCloud Servers	11
4.1	SAS 70/SSAE 16.....	11
4.2	Storage.....	11
4.3	Redundant Internet Connections.....	11
4.4	Backup and Restore	11
4.5	Uptime Specification.....	11
4.6	Security	11
4.7	Patch Management.....	12
4.8	Archiving of Access Logs.....	12
4.9	Service Availability Monitoring	12
4.10	Uninterrupted Power Supply	12
4.11	HVAC Support	12

1 Document Information

1.1 Purpose

The purpose of this document is to describe the Yubico YubiCloud Validation Service that provides cloud based (Yubico) OTP validation to customers in a convenient, secure, and reliable fashion.

The document describes both the service as well as supporting services for importing keys, production etc. and hosting environment for the service.

1.2 Audience

This document is intended for Yubico customers and partners wanting to use the reliable YubiCloud, cloud-based onetime password validation service.

1.3 References

No references to external documentation at this time.

1.4 Document History

Date	Ver	Author	Activity
November 8, 2011	1.0	Simon Josefsson Kurt Lennartsson	Initial Document

1.5 Definitions

Term	Definition
ISP	Internet Service Provider
KSM	Key Storage Module (Server for secure storage of AES keys)
YubiHSM	HSM AES Key Storage Module
OTP	One Time Password
UPS	Uninterrupted Power Supply
VAC	Ventilation and Air-conditioning

2 Introduction

Yubico (founded in 2007) is a two-factor authentication technology company with offices located in Sweden and England for Europe and Asia and in California for the North American market.

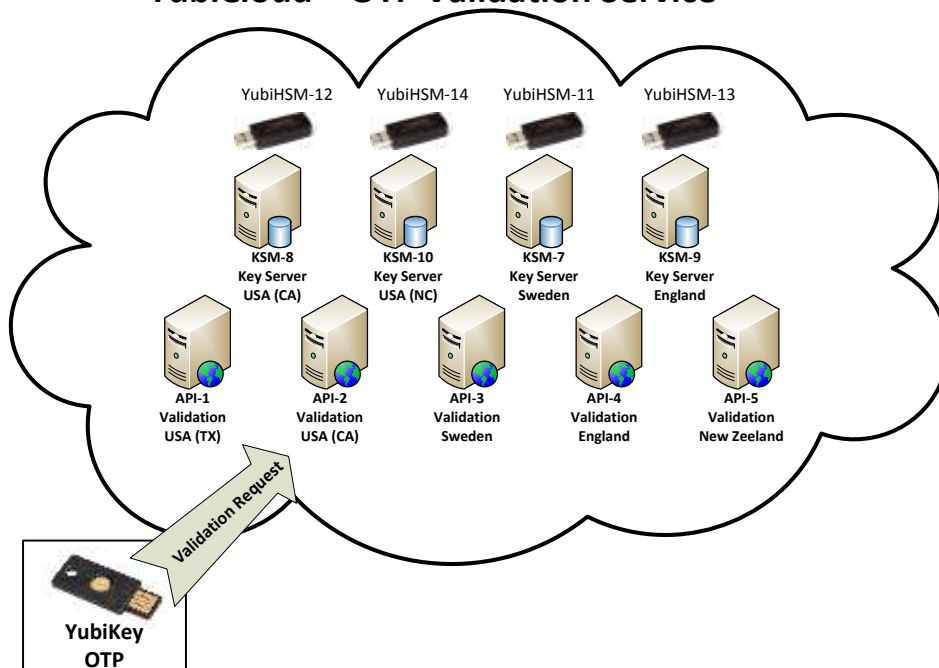
Yubico's mission is to "provide easy and secure login for everyone". The Company offers a physical authentication device/token, the YubiKey, which is used to provide secure two-factor authentication to web services and various other applications. The YubiKey device is a tiny key-sized one-button authentication device, emulating a USB keyboard and designed to generate a unique user identity and a one-time password (OTP) without requiring any software installed on the computer.

The company also offers open source software to customers or partners functioning as building blocks to provide or build secure authentication solutions.

Furthermore Yubico provides an online validation service which we will cover more in detail in the sections below. The YubiCloud is an Online Yubikey OTP 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 Yubico OTP online Validation Service. All geographical references and number of servers in this document are subject to change for operational reasons and is given for illustrational purposes.

YubiCloud – OTP Validation Service



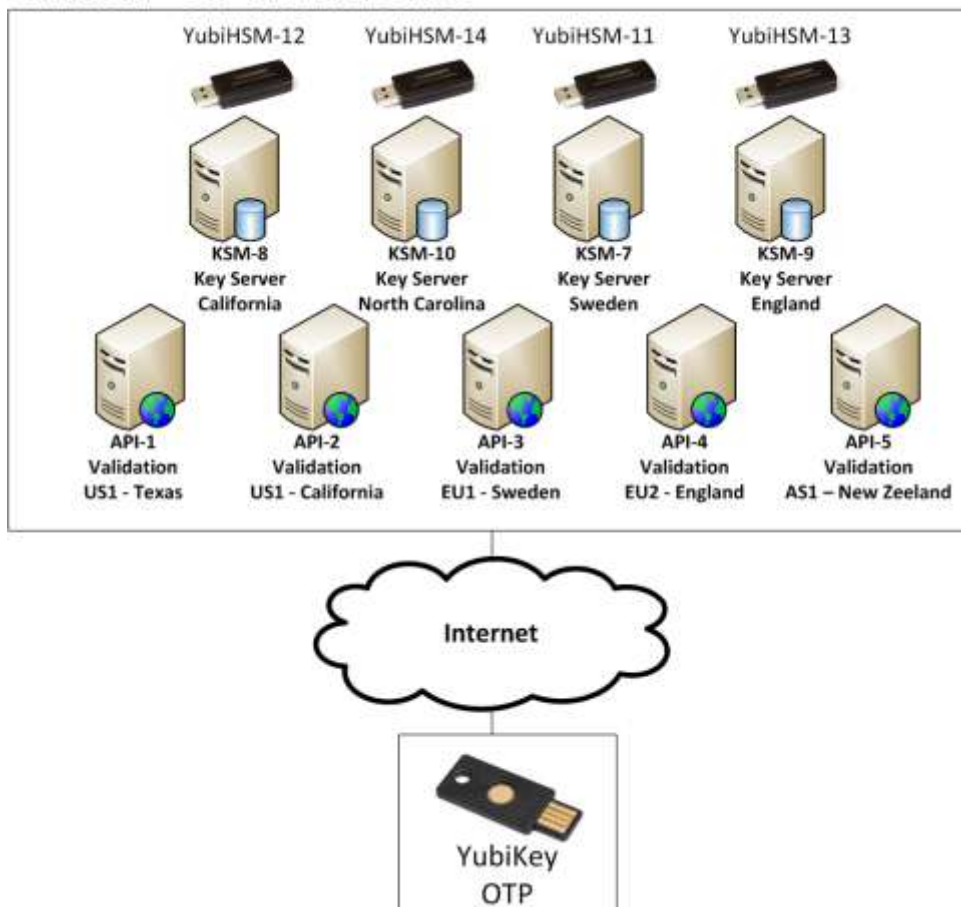
3 The YubiCloud

The YubiCloud free Yubikey validation service was launched march 2010 and the service has had almost 100% availability since launch (even though individual servers have been down, which is expected). YubiKeys normally comes ready to use with the YubiCloud (no programming of the keys required by the customer). The YubiCloud currently have a set of front end servers and a set of backend servers servicing the Yubikey OTP validation requests and they are all synchronized to each other making sure there is no single point of failure and that the validation responses are sent in a timely manner.

3.1 Redundant Services

The YubiCloud is a cloud based YubiKey One-Time Password (OTP) validation service. YubiCloud makes it easy to add first class two-factor authentication to your login environment, which may be a Web Service or even PC login. Our robust OTP validation servers are arranged in a distributed failover configuration at five different locations around the globe, all synchronized to each other making sure that there is no single point of failure and that responses are serviced in a timely manner, independent from where around the world validation request is sent. Each KSM backend server is equipped with YubiHSM Hardware Security Module(s) in order 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 administrations of the backend KSM servers.

YubiCloud – OTP Validation Service



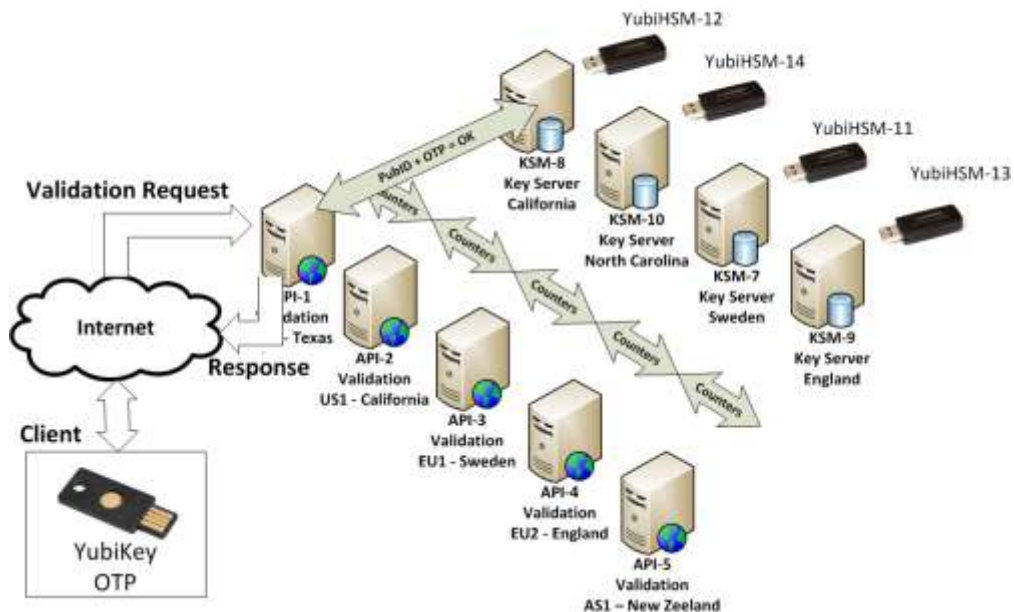
3.2 Validation Process

The validation process works by having the client send parallel requests to all YubiCloud validation servers. A parallel approach has two advantages: 1) Latency is reduced to a minimum since the client will not have to wait for the response that takes the longest to return, and 2) Availability is improved because even if several validation servers are unreachable from the client's network, validation will work correctly. Each validation server sends parallel requests to all KSMs in order to decrypt the OTP and will use the quickest response, also reducing latency while maximizing availability. Each validation server will also send 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 of the validation server software and algorithms, see the YK-VAL software documentation:

<https://code.google.com/p/yubikey-val-server-php/w/list>

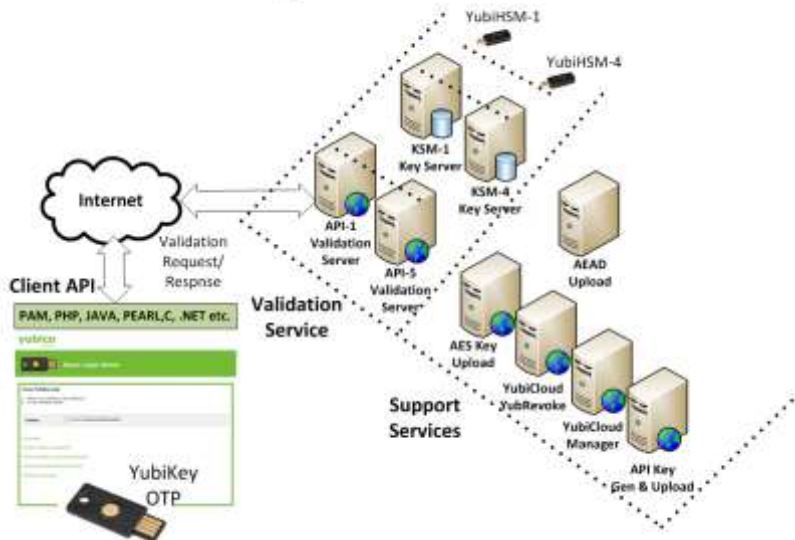
YubiCloud – OTP Validation Service



3.3 Components

YubiCloud service consist of core components for providing validation services (Validation Servers, KSMs and YubiHSMs) as well as supporting services such as key upload, YubiKey revocation service, API key generation.

YubiCloud – Components



3.4 Validation API software

To add YubiKey two-factor authentication to your application or Web Service through the YubiCloud validation service you can just use one of the client software and you will be up and running in a few hours (or less). See the following link for a list of some current client software:

<https://www.yubico.com/web-api-clients>

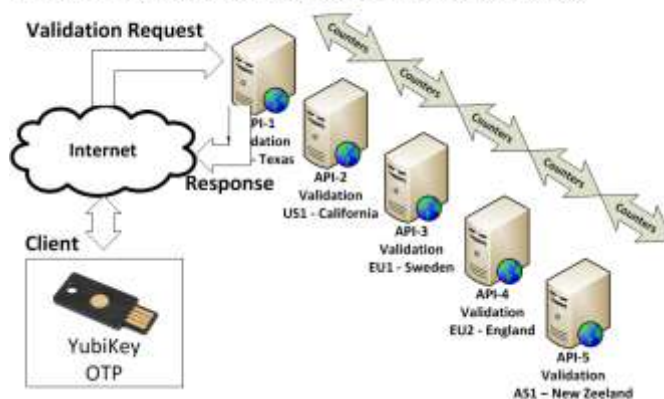
3.5 Sync between servers

The YubiCloud synchronizes the counters between servers. Below is a simplified picture for conceptual understanding of the sync process.

The details of the synchronization are available in the YK-VAL software documentation:

<https://code.google.com/p/yubikey-val-server-php/w/list>

YubiCloud – Sync of OTP counters between Validation Servers



3.8 AES Key Upload

Users are allowed to reprogram their Yubikey and may upload the AES key using our online web based interface. YubiKeys uploaded through this mechanism will always have to begin with 'vv' and it is not possible to remove or replace an AES key that is uploaded once.

<https://upload.yubico.com/>



The screenshot shows the 'Yubico AES Key Upload' web interface. At the top, there is a green header with the Yubico logo and the title 'Yubico AES Key Upload'. Below the header, a message reads: '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.' The form contains several input fields: 'Your e-mail address:' (with a placeholder 'email@address.com'), 'Serial number:' (with '547050'), 'YubiKey prefix:' (with 'vv#jpkgl'), 'Internal identity:' (with 'c0772e5e3b78'), and 'AES Key:' (with '88ef7190a7a0b0a300b10b1043c02'). Below these fields is an 'OTP from the YubiKey:' field with the value 'vv#jpkgl8337039a1a0a0a9q870'. A CAPTCHA image is displayed with the words 'ingsnaco' and 'whlqb' and the instruction 'Type the two words:'. At the bottom of the form is an 'Upload AES key' button.

The actual format of the upload is as follows.

<https://upload.yubico.com/?prefix=vvgkcfieckii&uid=8881b0e86658&aeskey=5c10650d82c9bbf187705afc7d3e7617>

3.9 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 a HMAC-SHA1 secret generated by Yubico.

<https://upgrade.yubico.com/getapikey/>

3.9.1 Management of API Keys

Users Manages the API keys. API keys are not managed by Yubico. If a user loses the API he/she will just create a new key.

3.10 YubiRevoke

YubiKey revocation service. Users may register their YubiKey(s) with the service and if one of the registered keys is lost or stolen the user may revoke the particular key. The service disables validation of the YubiKey on Yubico's validation servers only, and it is possible to reinstate operation of a YubiKey that has been disabled.

<https://admin.yubico.com/yubirevoke/login.php>

4 Hosting Environment for YubiCloud Servers

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

The Yubico Key Storage Module (KSM) are running on dedicated servers and each Key Servers has a YubiHSM attached which stores the KSM server encryption keys and performs that actual OTP decryption. Any penetration of the KSM server would not expose any AES keys.

4.1 SAS 70/SSAE 16

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 customers assurance on the design and operational effectiveness of those controls.

Even though at this time not all of the used hosting facilities used for hosting YubiCloud servers has the above certifications they have equivalent procedures in place.

4.2 Storage

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

4.3 Redundant Internet Connections

Servers are configured with 1Gbps LAN adapters connected to the internet through a set of redundant Switches and Firewalls to a multi Gigabit connection with failover capabilities providing speed and uninterrupted network access.

4.4 Backup and Restore

The Yubico Validation service backup process is configured to take full backup of the full database and application data on at least a daily basis to a remote server. Backups are transferred encrypted and are kept for at least one year. The software used is rsnapshot, see <http://rsnapshot.org/>.

4.5 Uptime Specification

The free Yubico validation service is offered on a reasonable-effort basis. We make an effort to resolve issues quickly, and is committed to offering the best service we can deliver. If you have special needs in this area, please contact us to negotiate a committed uptime guarantee.

4.6 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.

It provides:

1. 24x7 staff to provide monitoring against unauthorized entry
2. System installation is monitored to use latest upgrades
3. Firewalls to prevent unauthorized system access
4. Several CCTV security cameras monitor the data center 24x7
5. All cabinets and cages are locked, ensuring maximum security
6. Visitors are not permitted in server rooms
7. Maintenance work on machines is not permitted on-site to reduce security risks

4.7 Patch Management

The Yubico support team performs scheduled security patching of servers as required to ensure on-going system protection by applying patches to the operating system and all standard software modules used by Yubico OTP validation service in a timely manner. Since the nature of the YubiCloud service is that there is no single point of failure, server maintenance and upgrades are performed immediately when OS vendor upgrades are available. This may result in a few minutes downtime of a particular server but does not lead to any interruption of the YubiCloud service.

4.8 Archiving of Access Logs

The Yubico service provides secure archiving of all the important system and access logs to allow quick diagnostics of any kind of failure.

4.9 Service Availability Monitoring

The Yubico Support team are continuously monitoring the availability and performance of the Yubico OTP validation service and Yubico KSM using Nagios/Icinga monitoring software and through online monitoring service Pingdom. Customers may follow our incident reporting and uptime graphs on <http://status.yubico.com/>.

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

4.10 Uninterrupted Power Supply

The hosting facilities provides uninterrupted power supply along with backup power units to Yubico OTP Validation Server and KSM Server environment and other network/ system infrastructure.

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

4.11 HVAC Support

The facility provides Yubico Servers with HVAC that has redundancy to always maintain required temperature and environment for Yubico OTP Validation Service

The HVAC system has redundant chillers and multiple air conditioning units pumping cold air into the raised floor of the data center.

- Self-contained VAC units provide ample cooling power.
- VAC units carefully monitored daily by on site personnel.
- Raised flooring for optimal airflow.
- Humidity controller ensures optimal operation.