KeyTalk | Use Case Analysis

Canon-Oce network integration with Keytalk

KeyTalk.com

About KeyTalk

KeyTalk is an internationally operating Dutch software company that delivers complementary IT security solutions in strong authentication and secure data-in-motion protection. Our worldwide patented technology allows us to automatically and securely distribute and install digital short lived (X.509) certificates per second to any desktop computer, laptop, tablet, smartphone, or Internet of Things device. This results in a classic PKI-based security infrastructure but with less overhead and maintenance.

Certificates are used everywhere. From web servers (the lock in your browser) to client devices for secure authentication purposes. But managing certificates can be time consuming. KeyTalk's patented technology makes your business more efficient by replacing long (typically 1-5 year) digital certificates with short lived (typically less than 24 hour) certificates.

About Canon Océ

Canon Inc. is a Japanese multinational corporation specialized in the manufacture of imaging and optical products, including cameras, camcorders, photocopiers, computer printers and medical equipment. Its headquarters are located in Tokyo, Japan and was founded in 1937. Canon employs more than 190,00 people worldwide.

Océ is a global leader in digital imaging, industrial printing and collaborative business services. Its headquarters are located in Venlo, The Netherlands and was founded in 1877. Océ is active in over 100 countries and employs more than 20,000 people worldwide.

Since 2009, Canon and Océ have joined forces to create a global leader in the printing and imaging industry.

The Canon Océ use case

Canon-Oce has thousands of globally operating field engineers performing maintenance on Canon-Oce equipment. In order to properly perform this maintenance work, detailed information about equipment needs to be easily yet securely obtained from the corporate environment back at headquarters. This includes information such as blue prints and the availability of spare parts.

Oce-Canon is a very large company operating in hundreds of different countries. Newly acquired company network access regularly needs to be expedited in order to share company wide information.

The problem

Field engineers need secure VPN access from their computers. But when Wifi or 3G/4G disconnects these engineers often need to re-authenticate. Sometime up to 30 times a day.

Canon/Océ corporate policy demands strong authentication. But dirty hands or gloves are a burden when using a traditional smartphone app based or a physical one time password token based form of authentication. Additionally, having to re-authenticate numerous times a day creates a negative user experience and decreases efficiency. During lunch break computers tend to remain in the service vehicle. With smart cards still inserted and accounts authenticated, a stolen laptop from a vehicle becomes a security risk.

When an acquisition occurs IT department often need to provide access to and between different corporate networks. The acquired company might have one or more different types of strong authentication solutions; often with different network equipment vendors. Trying to tie all these different corporate networks together results is a loss in time and revenue.

Product Benefits

- **Provides advanced application and network protection for changing threats including Phishing, Man-in-the-Middle and Brute Force attacks**
- **Enables a wide range of secure wired, wireless and remote-access options**
- **Removes the maintenance burdens related to physical tokens**
- **Automatically re-authenticates when a connection is interrupted**
- **Streamlines security administration and lowers management cost**
- **Makes federated identity a reality**
- **Digital signing**
- **Corporate laptop & smartphone usage**

The solution

KeyTalk connects to multiple authentication solutions. As a result, any strong corporate authentication solution such as those provided by Safenet, RSA, Vasco, etc. can connect to KeyTalk. This results in a proof of identity with half a day validity (or variable length) client certificate.

Since the certificate is valid during the day, any Wifi or 3G/4G disconnect will simply result in a VPN re-authentication when network connectivity is available again. This allows the field engineer to continue his work without having to repeatedly re-authenticate.

By introducing additional device recognition, a multi-factor authentication layer is added to enhance security while also offering primary strong authentication for those offices not yet working with strong authentication.

Most importantly, the IT department doesn't need to configure newly acquired networks with a wide range of authentication solutions. They simply configure the network for X.509 certificate authentication; thereby making network access across all their offices a reality within days.

The benefits

When Canon/Océ introduced the KeyTalk certificate life cycle management engine, several clear benefits became apparent:

1) **Certificate and token management cost reduction**

Replacing the existing X.509 certificate was done in a non-automated fashion resulting in a high FTE count for management purposes. Calls to the internal support desk were reduced dramatically. This was a result of the KeyTalk solution being automated at almost every step; requiring virtually no technical knowledge whatsoever on the client side. Over time replacing traditional strong authentication tokens within Oce/Canon with KeyTalk's device recognition based strong authentication allowed for huge savings in costs.

2) Enhanced cyber security

- Automatically replacing certificates twice a day meant that a stolen device would no longer have had access to the network even if a thief had been able to login to the device.

- Thanks to KeyTalk's short lived certificates, there became no more need for the IT department to keep track of Certificate Revocation Lists (CRLs). This saved time by ensuring that certificates would never be forgotten to be revoked. And with it the potential abuse of lost certificates was fully negated.

3) **Improved scalability**

With KeyTalk supporting up to hundreds of millions of users, Canon-Oce was able to address staff growth without the overhead and hassles that come with using tokens. (KeyTalk offers at least the same level of client and device security as hardware tokens but with additional 2-face asynchronous encryption.)

4) **Leveraged interoperability**

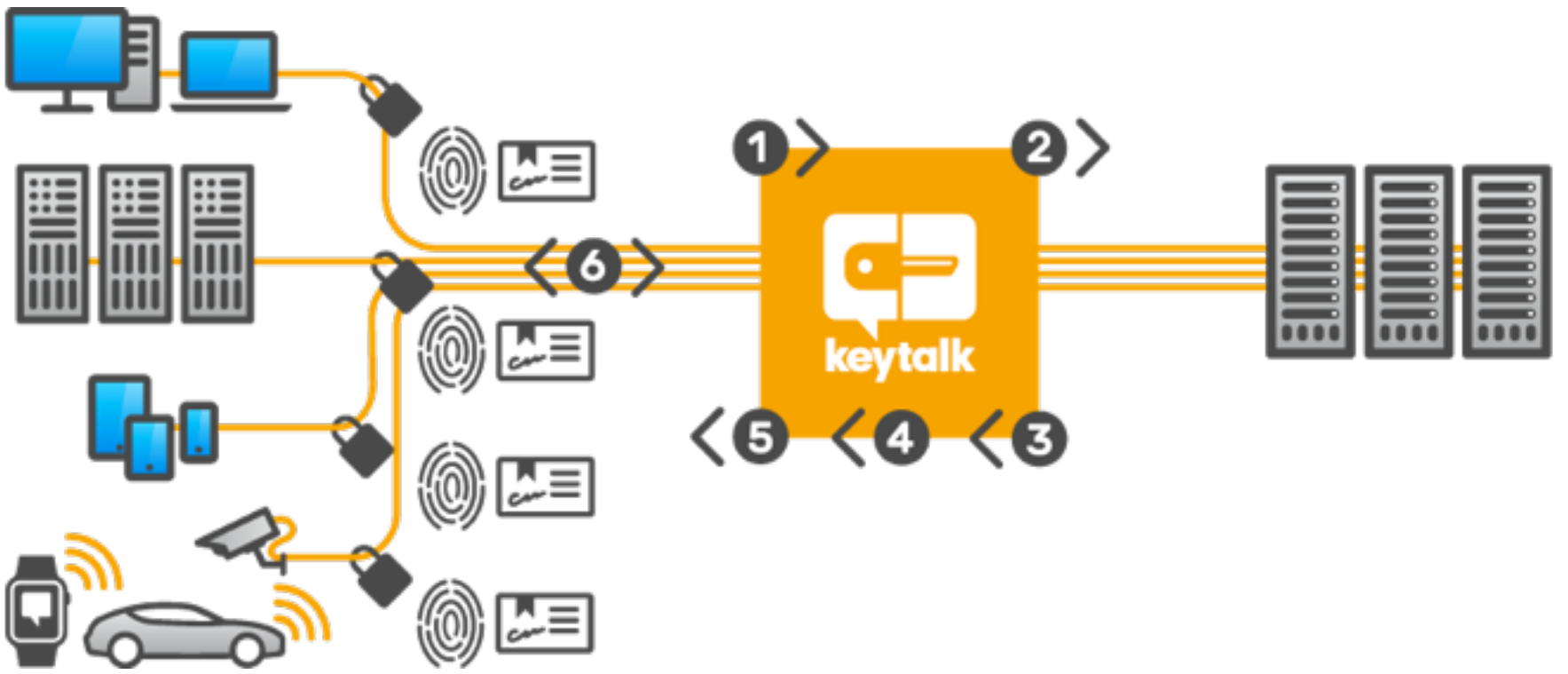
By using short lived X.509 certificates as a standard to access any of their network environments, the interoperability for the purpose of information sharing was greatly leveraged. This ensured anybody with a valid Oce-Canon issued client certificate could access the network areas they were authorized to.

By connecting the different authentication solutions, such as OTP generators, AD user/passwords and several others, all of these authentication methods were leveraged with device recognition as an added factor. This resulted in seamless information access by all users to any of Canon/Océ's networks by utilizing KeyTalk short lived X.509 certificates.

The implementation

Implementing KeyTalk tends to run smoothly. Most customers download our virtual appliance for VMWare from our website followed by the configuration of IP addresses and firewall rules. Then they walk through our Certificate Authority wizard. With a couple of clicks they have created a KeyTalk configuration file. Most customers are up and running with their own KeyTalk cluster in a couple of hours.

Generally speaking most of the work goes into configuring the network and finding a suitable procedure for installing the KeyTalk client/app. Network configuration, such as configuring a VPN for client certificates, takes a couple of minutes. Configuring multiple applications in complex network environments would clearly take longer. Finally, IT departments tend to remotely install the client to different devices or ask their staff to install it from the appropriate app store.



How does the KeyTalk infrastructure work:

1. The KeyTalk client (or SDK) triggers the authentication to obtain a certificate from the KeyTalk virtual appliance.
2. The KeyTalk appliance verifies the authentication credentials against the customer's authoritative source.
3. The authoritative source approves (or denies) the authentication.
4. KeyTalk verifies the hardware fingerprint of the device and creates the certificate and key-pair.
5. The certificate and key-pair are sent to the client device (such as an IP-camera, smartphone or laptop) from the KeyTalk virtual appliance.
   (In the background, the KeyTalk's client (or SDK) installs the obtained certificate and key-pair. And uninstalls the old one).
6. A highly secure connection is established between client and server by means of 2 way

info@keytalk.com | KeyTalk.com