Case Study

Strong VPN Authentication with KeyTalk

KeyTalk.com

The only way to properly secure access to your VPN is by using client certificates. So how do you securely obtain these certificates and manage vast amounts of them in your infrastructure? In order to keep the communications fully secure between your laptop, tablet, desktop computer, server and Internet of Things (IoT) devices with your target network, you should use a trusted valid client certificate.

Product Key Features

- IPv4 and IPv6 supported
- On-board high availability support
- RFC compliant standard X.509
- Short life validity for certificates
- New unique encryption keys with each issued certificate
- 1024 - 4096 bit RSA encryption keys
- Automated certificate processing
- Use existing authentication methods
- Optional trusted hardware recognition and management

KeyTalk Benefits:

- Provides advanced application and network protection for changing threats including phishing, man-in-the-middle and anonymous brute force attacks
- Enables a wide range of secure branch- and remote-access options
- Streamlines security administration and lowers management cost
- Makes federated identity a reality
- Corporate laptop and smartphone usage
- Machine to machine usage
- Internet of Things supported

VPNs and their vulnerabilities to phishing

Strong VPN Authentication is about authenticating to a VPN with more than just a username and password. It's about convenience for the end-user. Our VPN solution facilitates exactly that. Every company at some point provides a VPN connection for its staff. Whether its IPSec or SSL VPN, client based or client less. When implemented properly, a VPN ensures a secure connection between servers/networks and most commonly between a client and a network environment. Most VPNs remain connected as long as the connection is stable and data can be properly transmitted over it. For the most part, VPNs tend to be user friendly.

But there is a common misperception. While your network might be (or appear to be) securely accessible through a VPN, it doesn't necessarily mean that your VPN is providing the intended security. Most IT departments commonly have their infrastructure set up so their remote staff can authenticate to their VPN using a simple username/password and in some cases "One Time Passwords". A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system system or other digital device. OTPs avoid a number of shortcomings that are commonly associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication.

While OTPs are definitely a step in the right direction, static usernames/ passwords and OTPs are vulnerable to phishing. The window of vulnerability isn't that high in the case of OTPs and usually around 60 seconds. But 60 seconds is still long enough to be targeted by a well prepared spear phishing attacker. Phishing attempts directed at specific individuals or companies are called spear phishing. Potential attackers gather personal information about their target to increase their probability of success. This technique is without question the most successful on the internet today accounting for more than 90% of all phishing attacks. When phished successfully, a malicious party can simply authenticate to your VPN and access your corporate digital environment. Web-based VPN's are highly vulnerable to not only to phishing based intrusions but Man-in-the-Middle as well; thereby creating an even greater attack vector.

By using certificates for VPN authentication, KeyTalk provides "Single Sign on to the VPN".

As long as a certificate is valid and there is network connectivity, your VPN will re-initiate without having to manually re-authenticate.

With a valid certificate, the login procedure takes place only once.

Enhancing your VPN security and usability with KeyTalk

Companies who choose a Public Key Infrastructure usually do so for security reasons. A full blown PKI is simply a bridge too far for most companies but the level of security is still required. KeyTalk fills this gap between PKI and regular multi-factor authentication by providing short lived certificates that can have validity as short as a few seconds. It's the same technology compared to PKI, but without the huge overhead created by user certificate issuance, management and revocation lists. KeyTalk's certificates are obtained based on any form of authentication without the user even needing to know that they use client certificates.

KeyTalk's certificates are obtained based on any form of authentication without the user even needing to know that they are using client certificates. No administration is needed with a Certificate Revocation List (CRL). Furthermore, when using existing authentication solutions such as LDAP/AD or RADIUS based tokens, no management is required . Your IT department will be not only happier but more efficient.

The only way to properly secure access to your VPN and prevent Man-om-the-Middle attacks is by using client certificates. So how do you securely obtain these certificates and manage vast amounts of them in your infrastructure? In order to keep the communications fully secure between your laptop, tablet, desktop computer, server and Internet of Things (IoT) devices with your target network, you should use a trusted valid client certificate. With KeyTalk you can quickly and efficiently distribute many thousands of certificates to many thousands of devices in a matter of minutes. Thereby ensuring that your identity and your “electronic passport” is valid, up to date with the latest applicable credentials and fully secure.

Hardware recognition is of course nothing new. But most companies implement it using meta data coming from the browser. KeyTalk goes beyond browser meta data, making it near impossible for a malicious party to determine hardware recognition credentials remotely. Mac addresses aren’t sufficient since these can be easily spoofed. Keytalk uses multiple components definable by the Admn, such as BIOS Serial Number, HDD serial number, and many more, and as a result your hardware recognition will be unique compared to others using KeyTalk as well.

Using SSL certificates for VPN authentication purposes carries another huge benefit; namely "Single Sign On to the VPN”. While SSO offers a number of benefits, several SSO implementations are vulnerable to malicious attacks such as "cookie hijacking”. Cookie hijacking, or session hijacking, is the exploitation of a valid computer session—sometimes also referred to as a session key—to gain unauthorized access to information or services in a computer system. This is not the case with short lived certificates issued based on strong authentication where KeyTalk ties a user’s authentication to that user’s (pool of) corporate approved trusted devices, whereby the device hardware fingerprint is used. More often than not a remote and/or traveling employee finds his or her VPN connection terminated due to losing their wifi, 3G or 4G connection. Work and time is lost and frustrations increase. And they must, yet again, authentication with their VPN to get access back to their network/server. Here’s where our “Strong VPN Authentication” solution shines. As long as a certificate is valid and there is network connectivity, your VPN will re- initiate without having to manually re-authenticate. Saving a lot of annoyances client side from your traveling staff without having to compromise corporate security protocols.

KeyTalk is better and easier to manage than tokens.

X.509 certificates are the login method to applications such as SAP or Sharepoint.

KeyTalk can evolve into a Single Sign On to all corporate applications.

With a valid certificate, the login procedure takes place only once.

Clientless VPNs and the risk of MitM attacks

Web-based VPN's are highly vulnerable to not only to phishing based intrusions but also Man-in-the-Middle attacks which creates an even greater attack vector. KeyTalk strives to eliminate any chance of Man-in-the-Middle attacks with our "Strong VPN Authentication" solution. End-to-end encryption ensures that data is transferred securely between endpoints. An eavesdropper may impersonate a message recipient (during a key exchange or by substituting their public key for the recipient's), so that messages are encrypted with a key known to the attacker. After decrypting the message, the snoop can then encrypt it with a key that she shares with the actual recipient, or his public key in case of asymmetric systems, and send the message on again to avoid detection. This is known as a man-in-the-middle attack.

Most cryptographic protocols include some form of endpoint authentication to prevent MITM attacks such as certification authorities or webs of trust. An alternative technique is to generate unique one-time strings of characters based on the communicating users' public keys or shared key. The parties compare their phrases using a trusted communication channel before starting their conversation. If the characters match, there's no man in the middle. It's also worth noting that a users' computer can still be hacked, their cryptographic key can be stolen or the recipients' decrypted messages can simply be read. Even the most perfectly encrypted communication pipe is only as secure as the mailbox on the other end. That's why using KeyTalk's SSL certificates for VPN authentication are your best bet for avoiding attacks.

Clientless VPNs allow end users to securely access a corporate network from anywhere using an SSL-enabled Web browser. Clientless SSL VPN creates a secure, remote-access VPN tunnel to a Web browser without requiring a software or hardware client. It provides secure and easy access to a broad range of Web resources and both web-enabled and legacy applications from almost any device that can connect to the Internet via HTTP. clientless VPNs, which are effectively a HTTPS website based connection, are also vulnerable to man-in-the-middle attacks; in particular when used over a public and insecure Wifi connection. Enforcing client certificate based authentication to these SSL VPNs resolves the issue of MitM.

KeyTalk is better and easier to manage than tokens.

X.509 certificates are the login method to applications such as SAP or Sharepoint.

KeyTalk can evolve into a Single Sign On to all corporate applications.

With a valid certificate, the login procedure takes place only once.

Our solution

KeyTalk is a (virtual) appliance based product which seamlessly fits into your existing network infrastructure. It automatically creates, distributes, and (de)installs, short-lived X. 509 user certificates with corresponding cryptographic key-pairs.

Since the 1980's, X.509 has been the industry standard and is supported by all major network components and enterprise application solutions. This makes it the perfect unified access control solution.

Managing X.509 certificates has been one of the large cost factors (in both administrative and financial) in high secure environments.

Certificate management with the KeyTalk product line allows you to re-use your existing authentication environment. It can also be leveraged with KeyTalk's trusted corporate and BYOD (bring your own device) recognition. Furthermore, this reduces the lifecycle of the certificate and ultimately automates the certificate requests, creation, distribution and (de)installation.

KeyTalk secures the sending of user authentication credentials, enables encrypted access to the network to the highest level and protects against harsh attack vectors such as man-in-the-middle and brute force. Administrators will have less work on configuring networks for different types of authentication. End-users will save time and become more productive thanks to single sign-on to applications and network environments.

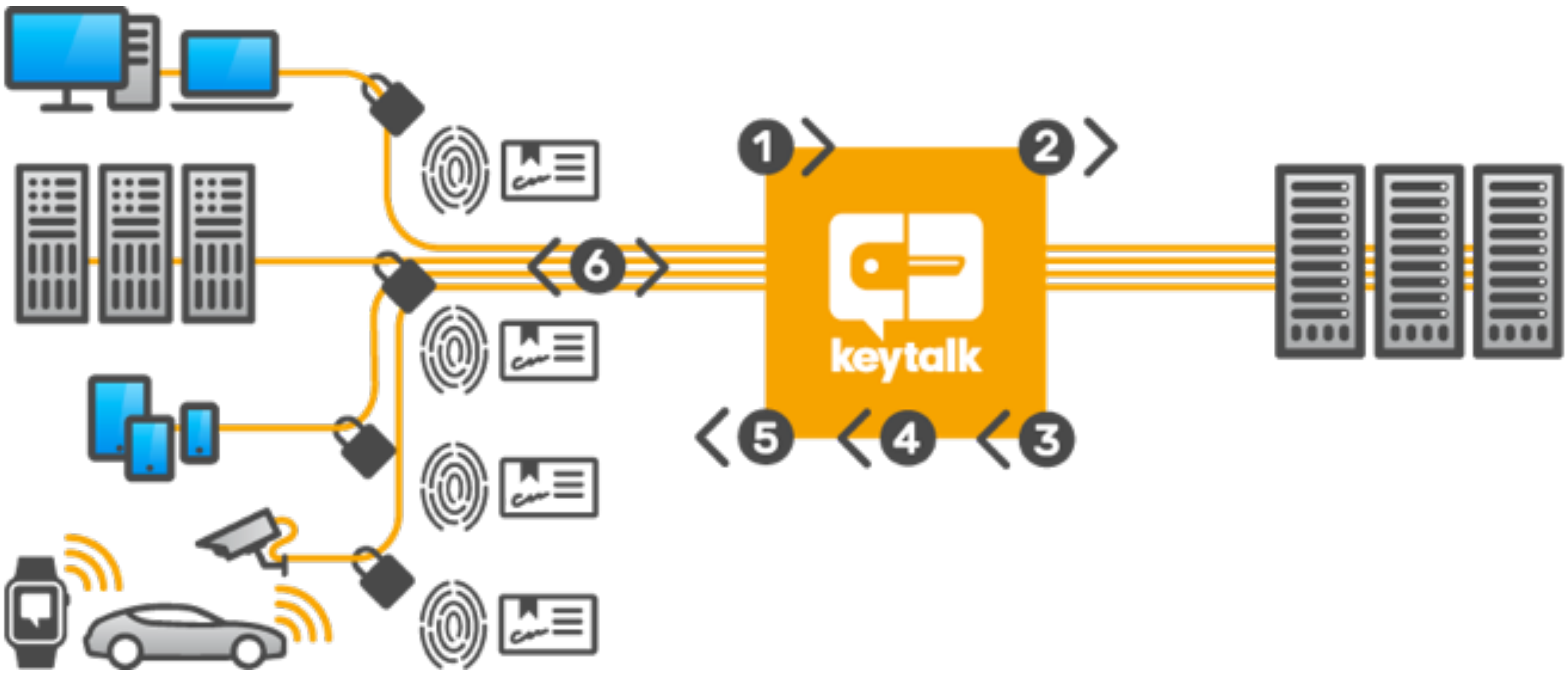
KeyTalk is the industry's most secure, easy to implement,
manage and use client certificate solution

Industry practical applications

The most common use of KeyTalk is to identify your trusted employee and partner devices to conveniently yet securely access your corporate applications. Often in combination with the existing product lines of HP, Palo Alto, Cisco, F5, CheckPoint, Juniper and others.

Smartphone app developers are regularly confronted with their app data-stream and app-server getting hacked. Fortunately, the KeyTalk API can be efficiently utilized as your security module in your app.

Secure app and Internet of Things communications is a necessity nowadays as well. Examples include vending-machines communicating their daily sales, ATM's communicating wirelessly with the bank, IP-camera's securely sending their video feeds, medical devices sending privacy sensitive patient data to online patient dossiers, and much more. KeyTalk fits right in and can handle it all. Be it for dozens or even hundreds of millions of users and devices.



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 SSL certificate authentication.

KeyTalk client and available SDK for:

Client platforms	Windows 7, 8, 10 Server 2008 / 2012 Citrix iOS Android BlackBerry 10 Windows Phone (Q4 2015) MacOSX Linux IIS 7 Apache
Client SDKs for embedded software integration	Yes

KeyTalk 4.x and DevID 1.x:

Authentication solution modules	Active Directory / LDAP RADIUS MySQL
Authentication solution modules external	Any authentication backend supported API based
Existing CA supported	Yes, as a sub-CA
Certificate key length	1024 bit RSA for legacy purposes 2048 bit RSA 4096 bit RSA Up to 521 bit ECC 2016
IPv4 support	Yes
IPv6 support	Yes
High availability	Yes
Dimensions	1U (356mm depth)
Power	260 Watt PFC
LAN	3 NIC's Internal External Management
Warranty	Hardware 2 years (does not apply for Virtual appliance)
Certification	CE certified
LED message display	Yes
User device identification	Yes
Trusted devices per user	10
Virtualization	Yes, OVF format for VMWare
Average implementation time	3-5 day

keytalk

KeyTalk.com