Case Study

Securing applications

KeyTalk enhances security for SAP, Salesforce, Exact, AFAS and other applications

KeyTalk.com

KeyTalk delivers an online access solution that is easy to use and administer and adaptable to your constantly evolving application landscape. Our "Secure Connect for Applications" solution provides the highest level of security possible for applications such as SAP, Salesforce, Exact and others without physical tokens or software generators. KeyTalk securely and automatically issues short-lived client and server certificates, based on a combination of device recognition and regular authentication, for highly secure mutually authenticated SSL connection purposes. (Attributes of the certificate are used to login to a target applications such as SAP.)

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 your existing authentication methods
- Optional trusted hardware recognition and management
- Runs also under your existing CA

KeyTalk Benefits:

- Offers automated short lived certificates installation for desktop, laptop, tablet & smartphone.
- 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 costs
- Secure, cheaper and complementary alternative to hardware tokens
- Makes federated identity a reality

keytalk

Keeping applications secure

Staff are increasingly working outside their office network environment but still require a safe mechanism to securely authenticate back to their ERP and other systems. And their local IT administrators need the ability to quickly and efficiently facilitate that. No one wants to waste time using tokens and multiple log in procedures.

KeyTalk securely and automatically issues short-lived client and server certificates, based on a combination of device recognition and regular authentication, for highly secure mutually authenticated SSL connection purposes. This is easy to use, inexpensive and scalable. With a valid certificate, the login procedure takes place only once. And simple Single Sign-On to all corporate applications is a reality.

Innovative new ways to attack enterprise applications in the cloud or on the corporate network are constantly on the rise. And they are becoming more sophisticated. At the same time, application and network requirements are growing more complex. Users are increasingly accessing assorted ERP and CRM solutions over networks that are not secure and/or through apps.

Software applications such as SAP, Salesforce, Exact and others contain sensitive and private data that needs to remain out of the hands of cyber criminals. Threats such as phishing, Man in the Middle and brute force attacks need to be protected against. Using KeyTalk solutions makes it much harder for hackers to attack your systems.

To take full advantage of Internet and cloud infrastructures, enterprises must be able to guarantee both the security of business communications and the protection of internal resources. Enterprises also need to address the challenges of availability, performance, and scalability for mission-critical applications while still allowing for user and administrator convenience.

KeyTalk is the only security technology manufacturer in the world, capable of seamlessly distributing hundreds of millions of short-lived digital certificates and corresponding encryption key-pairs per day.

Benefits:

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.

21st century security challenges

The European Data Protection Reform has been recently approved (January 2016) and will affect the range of the General Data Protection Regulation and the Data Protection Directive. Simply put, companies dealing with private and sensitive information are required to take appropriate security measures to prevent data leaks. If these security measures are not taken, significant fines will be incurred up to 10% of your company group revenue. Let KeyTalk help you comply with this important EU legislation.

Our technology provides a second or third factor of security (via trusted devices) that enables a two way SSL authenticated connection that is encrypted. And it is the most reliable method using automatically managed short lived certificates and changing encryption keys. You can also seamlessly integrate your existing application infrastructure using our KeyTalk Software Development Kit (SDK). Finally, the multi-tenant KeyTalk (virtual) server can run in your own network or be used from the cloud as offered by KeyTalk service provider partners.

SHORT LIVED CERTIFICATES STRONG AUTHENTICATION TRUSTED DEVICES

keytalk

Secure Communications

When organisations need to provide their staff and unmanned devices to (temporarily) cooperate together, secure communication becomes key.

Using symmetric encryption ensures the lowest overhead but doesn't help you determine if a data package got sent from a trusted source.

A-symmetric encryption using the X.509 standard, is perfectly suitable for verifying a data package or data stream came from a trusted source, but traditionally comes with high administrative overhead.

KeyTalk enables you to use your existing PKI infrastructure, or create on-the-fly a new Certificate Authority, and distribute to any amount or type of devices temporarily valid X.509 certificates. It is trustworthy and invokes strong data-in-motion encryption without classic PKI overhead.

More 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**
- **Streamlines security administration and lowers management costs**
- **Makes federated identity a reality**
- **Digital signing**
- **Internet of Things usage**
- **Server usage**
- **Corporate laptop & smartphone usage**
- **Strong a-symmetric keys 2048-4096 bit RSA, and per Q3 2016 up to 521 bit ECC**

Your digital identities

KeyTalk also protects your client and server authentication against malicious third party Man-in-the-Middle intrusions.

Based on our patented automated secure mass distribution of short lived industry standard X.509 certificates, your communication is securely enabled to mutually SSL authenticate to your secured network. It uses state-of-the-art periodic changing a-symmetric encryption key-pairs. You can also use it to encrypt and sign data packages.

Each time a new certificate is securely requested by your user using KeyTalk, KeyTalk will automatically pick-up on your device's user identity, or device identity credentials and embed them in the issued short lived X.509 certificate. This allows you to utilise your user's identity information in any way you see fit to your target network.

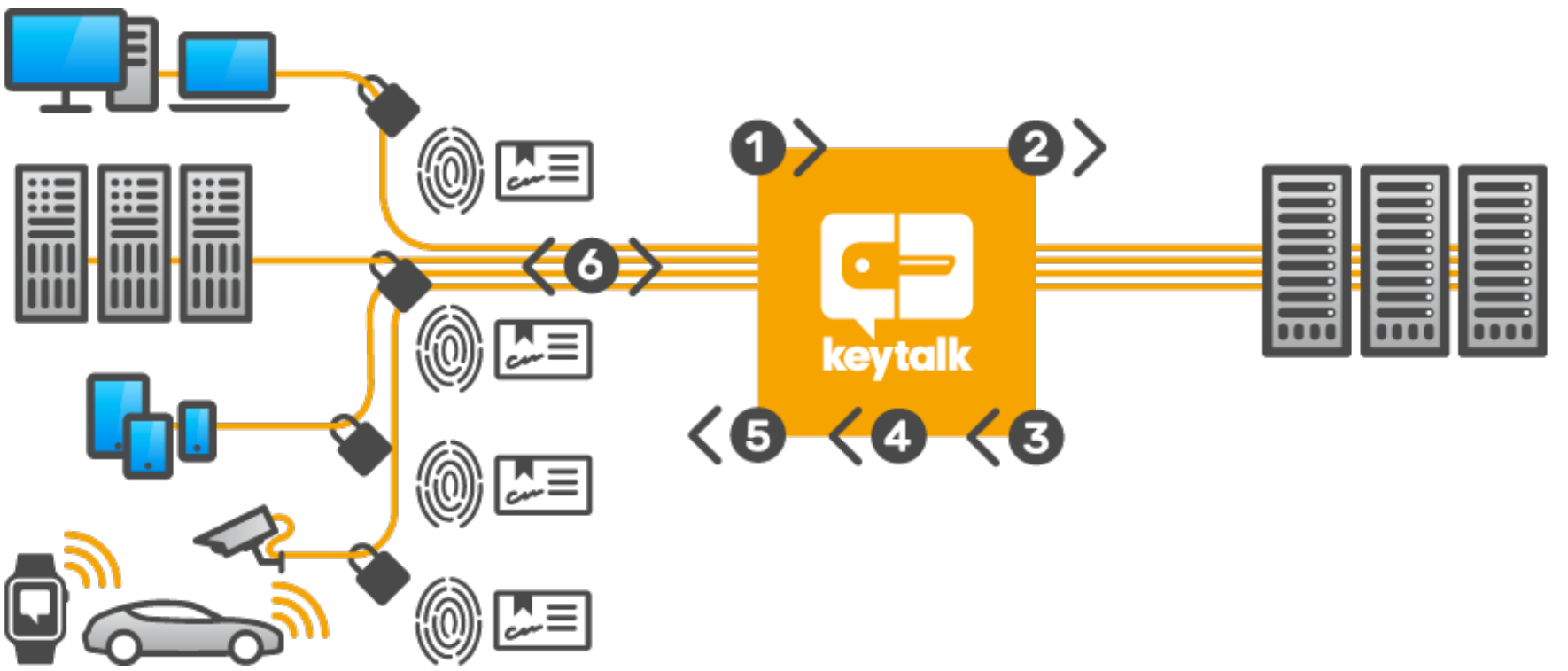
Best of all, KeyTalk allows the admin the change key-length and applied algorithm (RSA versus ECC) on-the-fly; thereby ensuring the most optimal key-length at any given time for the purpose you have envisioned.

Because X.509 is a standard and KeyTalk issues short-lived certificates, you can leverage interoperability between groups of people or devices for a short or longer period of time.

Get in touch with KeyTalk to hear more.

How does the KeyTalk infrastructure work:

1. The KeyTalk client (or SDK) triggers the authentication to obtain a certificate from the KeyTalk virtual appliance when no valid certificate is present.
2. The KeyTalk appliance verifies the authentication credentials against the customer's authoritative source, such as AD, LDAP, RADIUS, MySQL etc.
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, server, 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 over TLS or SSH.



info@keytalk.com | KeyTalk.com