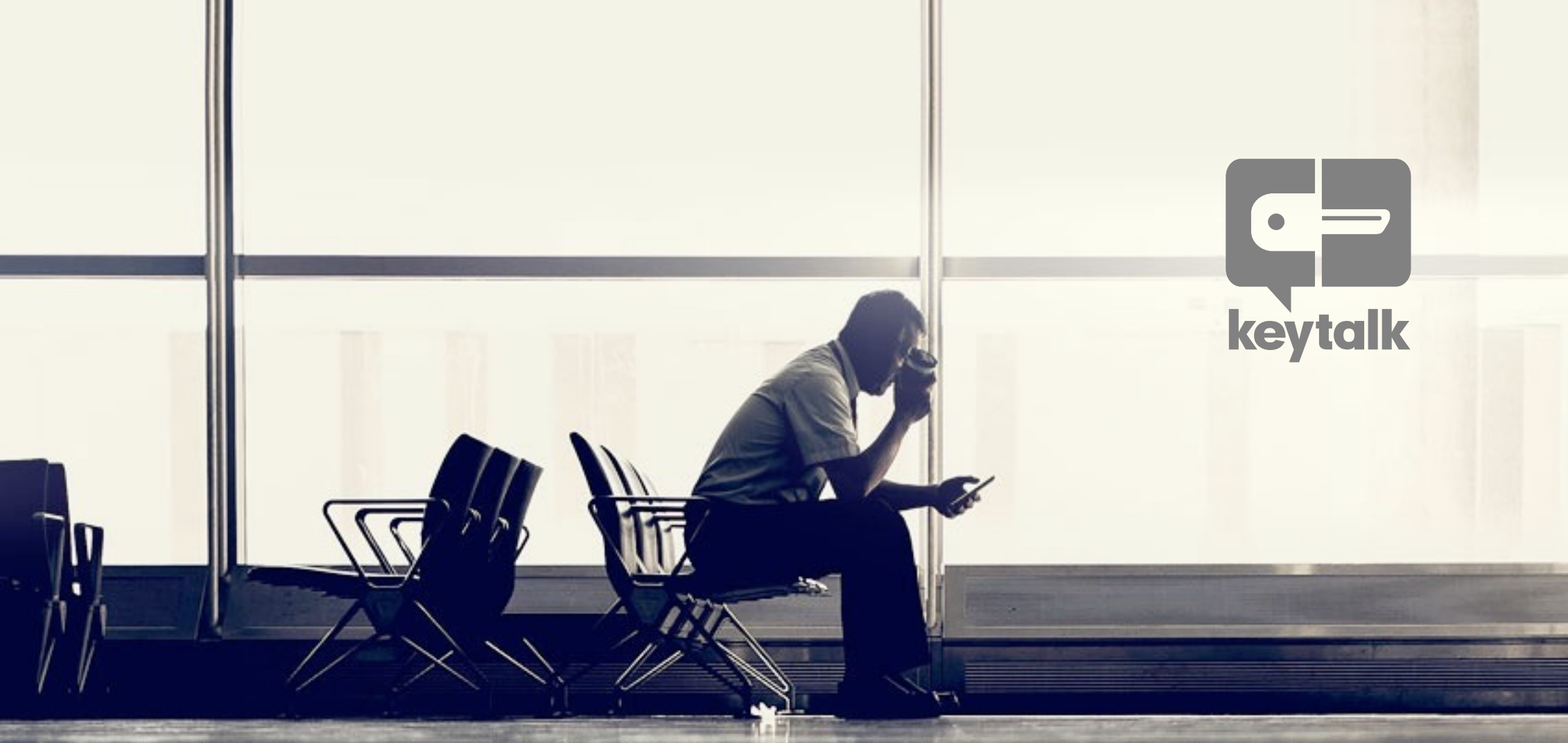


Case Study | Internet of Things

Protection against Cyberattacks

Security in the Internet of Things

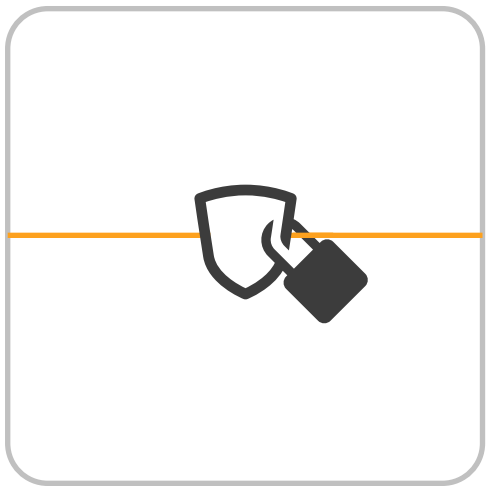
KeyTalk.com

KeyTalk and Security in the Internet of Things

These are exciting times for the wireless Internet of Things (IoT) industry. Around the world, billions of IoT connections are revolutionizing the way that companies do business. Across a broad range of sectors, significant gains are being made thanks to the promise of the Internet of Things. The possibilities are endless. And innovations are being made in industries as diverse as healthcare and utilities to automotive and agriculture.

KeyTalk is a convenient highly secure product which helps protect your IT infrastructure, whether a stand-alone network or in a cloud, against advanced Internet and network based threats.

As the industries and devices increase, the security of these connections will be of paramount importance. As a result, network operators need to work with dedicated security providers that can integrate with their existing network platforms. And they need provide protection that bridges the gap between legacy ‘human-to-human’ standards of protection and those required for M2M.



Your Machine becomes a token

KeyTalk protects the Internet of Things ecosystem against Man-in-the-Middle and Phishing attacks. Based on our patented and automated distribution for short lived machine certificates and unique crypto keys, machines transfer data to servers and the cloud from their KeyTalk identified trusted machines. They use state-of-the-art short lived encryption keys that require virtually zero management and administration. KeyTalk identifies the machines based on their hardware footprint. This is an additional authentication factor on top of the one you already have.

Though considered by many as a break-through innovation in the application and industrialization of PKI based technology, it’s still based on de facto security standards thus compatible with any network, just with less overhead, cost and management effort.

Securing sensitive data in motion without overhead

With KeyTalk, machines you trust can securely connect to target servers, or each other, over any non-secure network or the internet; be it via cable, cellular or WiFi.

All that is required is for your server to be trusting your KeyTalk instance as a trusted source and you are good to go.

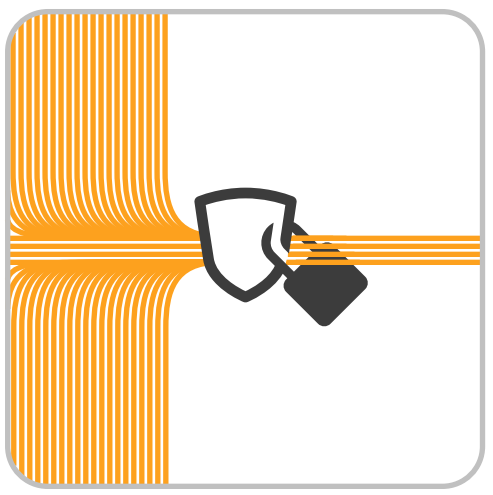
Due to using short-lived certificates the need for classic high overhead and maintenance PKI revocation pointers become a thing of the past.

Threats and compliance

Many security specialists will confirm that Man-in-the-Middle attacks nowadays are a viable risk. Not only on commonly used WiFi connection, but also on cellular networks.

While regular voice calls on the cellular network are still hard to maliciously intercept, using for example an IMSI catcher, the data streams using 3G/4G are an easy target. Consequently, they require additional encryption on top of the encryption already provided by the cellular network.

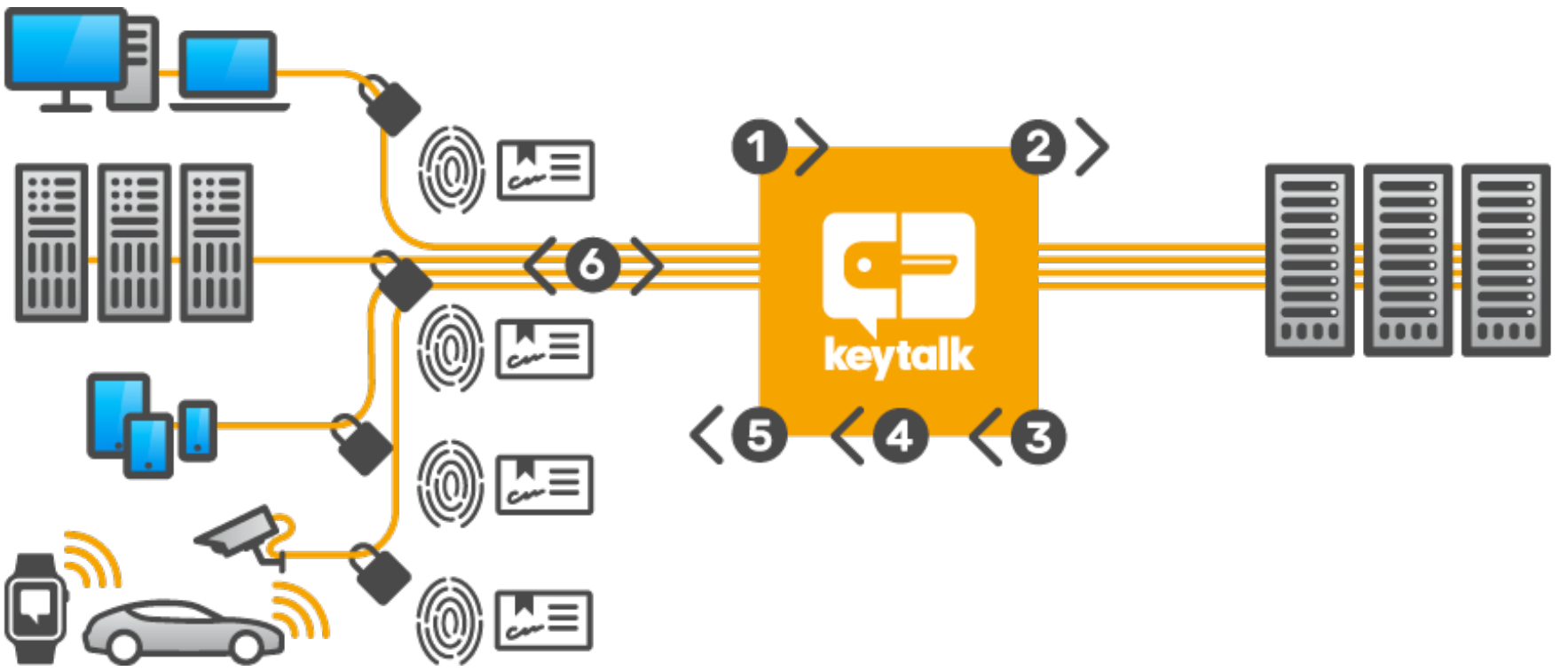
In 2016, the European Data Protection Reform will require companies dealing with private and sensitive information to take appropriate security measures to prevent data leaks. If these security measures are not taken not, significant fines will be incurred up to 2%-5% of your company group revenue. Let KeyTalk help you prepare for this important EU legislation.



KeyTalk recommends introducing strong a-symmetric encryption keys and corresponding X.509 certificates to both your Internet of Things network and your server network. When using KeyTalk's patented secure distribution mechanism, you will have the strongest possible level of encryption for your Internet of Things infrastructure. All without overhead on your M2M CPU in regard to key-generation.

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**
- **Streamlines security administration and lowers management cost**
- **Makes federated identity a reality**
- **Digital signing**
- **Internet of Things usage**
- **Corporate laptop and smartphone usage**
- **Strong a-symmetric keys 2048-4096 bit RSA, and per Q1 2016 up to 521 bit ECC**



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.

info@keytalk.com | KeyTalk.com