KEYTALK 5 CKMS

Secure automated Certificate & Key Management and enrolment Solution

The Challenge

Every company deploys PKI certificates. Often to ensure HTTPS on their websites, but also in many more applications such as strong client VPN authentication, WIFI authentication, and/or email encryption (S/MIME).

Admins often lack the proper tools to keep track of what certificates reside within their network, and especially outside of their network. It's not uncommon to keep track of certificate expiry by means of a calendar reminder or an Excel sheet, and more often than not these tracking methods fail.

Even when an Admin starts the certificate replacement process on time, it's usually a lengthy process: generate a Certificate Signing Request, request the certificate at your internal CA or Trusted Certificate Provider, obtain the certificate, and (often the hardest part) getting the certificate installed and activated in the proper location on the target device.
Just think about your road-warrior staff or business partners in remote areas with their laptops, tablets and smartphones? Your servers in other countries? How about Internet of Things devices, IP cameras, sensors, SCADA systems?

KeyTalk brings a secure scalable affordable solution to tackle these certificate management and enrolment challenges. Your Admins have fewer worries, can focus on more important things, and your company complies with relevant regulations in a timely manner. Your IT network becomes simply more secure and compliant.

Our Solution

KeyTalk 5 is a virtual appliance based solution, which fits seamlessly into your existing network infrastructure. It automatically creates, distributes, and (de)installs, short-lived or long-lived X.509 certificates with corresponding strong cryptographic key-pairs, securing server, user & device connections.

Authentication of an end-point relies on the authentication solution you currently have in place. Active Directory (incl Kerberos), LDAP, Radius, MySQL etc.
In addition, we optionally allow for additional trusted hardware verification on top of the authentication solutions you choose to connect to KeyTalk.

Host KeyTalk yourself or ask your trusted partner to host it for you. It's your choice; the KeyTalk solution allows you to serve from single up to hundreds of millions of end-points with certificates automatically replaced on a Just-in-Time basis.

Unlike our competitors, we do not rely on the Microsoft network domain certificate distribution methodology, nor do we rely on email clients or Mobile-Device-Management solutions. These are simply too limiting, requiring you to implement multiple solutions to cover all your user devices, servers and IoT devices.

KeyTalk 5 not only brings its own private CA to the table, allowing for dynamic certificate profiles, but it's CA-source independent as well.

Issue your certificates not just from the KeyTalk private CA, but in parallel from Trusted Certificate Service Providers, such as GlobalSign, Sectigo and QuoVadis. Or private CA solutions such as your Microsoft CA and PrimeKey.

When you wish to change a CA source, simply flip a switch within KeyTalk 5, all without hampering your served end-points no matter where they are located.

KEYTALK 5

Product description

KeyTalk 5 is a Certificate Authority vendor neutral, certificate & key-pair management and enrolment solution.

It just-in-time automatically requests, securely enrols and (de)installs X.509 certificates from any trusted CA source to any server, client device, and IoT device.

Our stand-alone SSL/TLS certificate discovery solution helps you find all your certificates and potential vulnerabilities in your network

Product Key Features

- ISO 11770-1:2010 principles
- RFC compliant standard X.509
- Key & certificate roll-over support for S/MIME and Bitlocker purposes
- Hardened S/MIME address book
- SHA2
- 2048 - 8192 bit RSA encryption keys
- Up to 521 bit ECC ready
- Automated CSR generation processing
- Secure client self service
- Use existing authentication methods
- Optional trusted hardware recognition and management
- 3rd party HSM support
- 3rd party key management support
- KeyTalk private CA
- 3rd party private CA support
- Primary (Qualified) Trusted Certificate Service Provider support
- Secondary (Qualified) Trusted Certificate Service Provider support

Product Benefits

- Eliminate expired certificates on end-points KeyTalk manages
- Enable advanced application and network protection for changing threats including Phishing, Man-in-the-Middle and Brute Force attacks
- Enable a wide range of secure branch/remote access options
- Streamline security administration and lower management costs
- Make federated identity a reality
- Works independently of the network

KeyTalk 5 CKMS facts

Client support	
End-point	✓ Windows 7, 8, 10 (including TPM 2.0) ✓ Windows Server 2008 / 2012 / 2016 ,incl Citrix & Remote Desktop ✓ IIS 7, 8, 10 (including SNI) ✓ iOS ✓ Android ✓ MacOSX ✓ Linux (Ubuntu, Debian, RHE, and more) ✓ Apache ✓ TomCat
REST API	✓ Yes
Client OpenSource	✓ Yes
IoT support	✓ Yes

Virtual appliance	
Operating System	✓ Ubuntu 16.04 LTS
High Availability Db	✓ MySQL 5.7.8 and beyond
Virtualization	✓ Yes, VMware, HyperV, Azure, AWS
IPv4 / IPv6 support	✓ Yes
Community size supported	✓ 1 up to hundreds of millions
Multi tenant	✓ Yes
Management roles	✓ Yes
Self-Service portal	✓ Yes
Internal private CA	✓ Yes
3rd party private CA support	✓ Yes
Partnered TCSPs	✓ GlobalSign ✓ QuoVadis (incl PKI Overheid) / Digicert ✓ Sectico (Comodo) ✓ TrustCubes
Secondary TCSP support	✓ Yes
Certificate key length	✓ 2048 – 8192 bit RSA ✓ Up to 521 bit ECC ready
Network independent	✓ Yes
IDP supported modules	✓ Active Directory / LDAP ✓ Internal MySQL Db ✓ MySQL ✓ RADIUS ✓ REST
Certificate publication	✓ Active Directory ✓ LDAP
External HSM support	✓ Yes
External Key Management support	✓ Yes
Certificate and Key roll-over (SMIME, Bitlocker etc)	✓ Yes
Key-roll-over private key encryption	✓ Yes, AES 256
Device identification	✓ Yes
Stand-alone S/MIME address book	✓ Yes (up to 50.000.000+ users)
Certificate discovery	✓ Yes (dedicated virtual appliance)

KeyTalk company	
Public status	✓ Privately owned, 100% Dutch
Support	✓ 24 / 7

Contact us at: sales@keytalk.com