keytalk

Product Fact Sheet

Simply the **Best PKI Management Platform** in the World

sales@keytalk.com • www.keytalk.com

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 CKMS is a virtual appliance based solution, and is offered as a hosted service as well, KeyTalk CKMS is a virtual appliance-based solution and is also offered as a hosted service, seamlessly fitting 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 CKMS 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 your Microsoft CA as well as from publicly Trusted Certificate Service Providers, such as GlobalSign, DigiCert, and Sectigo. When you wish to change a CA source, simply select a checkbox within KeyTalk CKMS, all without hampering your served end-points no matter where they are located.

The KeyTalk solution suite also provides network certificate discovery, and LDAP based S/MIME address book functionality.

SOME OF OUR CUSTOMERS

TKE

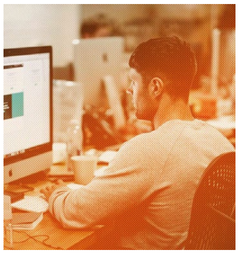
TenneT

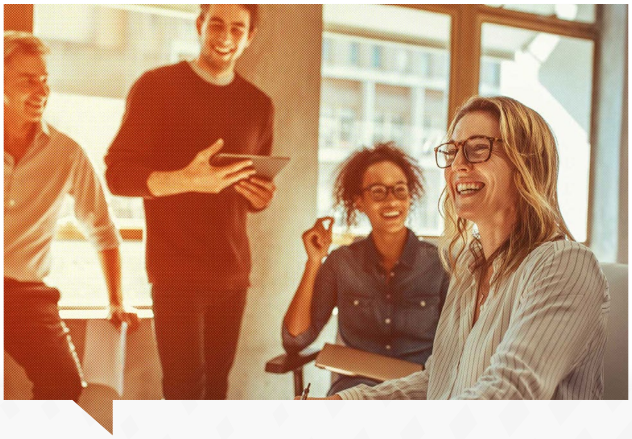
CYMOTIVE TECHNOLOGIES

CONET

financeinmotion

Struggling with PKI Management?





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

It just-in-time automatically requests, securely enrolls 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.

TLS/SSL Certificate LifeCycle Management (CLM)

By automating TLS/SSL Certificate LifeCycle Management (CLM) with Keytalk CKMS, you prevent risks associated with human errors and save a lot of time and resources to CLM.

Secure Email Service (SES)

The ideal first line of defense against Business Email Compromise (BEC/EAC). S/MIME certificates can be easily requested, deployed, installed, and configured for use.

Device Authentication (DA)

Secure authentication to networks (VPN/WIFI) and applications is crucial. Managing personal X.509 certificates for device authentication based on 802.1X ensures this.

KEY FEATURES

- ✓ ISO 11770-1:2010 applied principles
- ✓ RFC compliant standard X.509
- ✓ Key & certificate roll-over support for S/MIME and other purposes
- ✓ Hardened S/MIME address book
- ✓ 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
- ✓ (Qualified) Trusted Certificate Service Providers, such as DigiCert, GlobalSign, Sectigo

KeyTalk CKMS Facts

Laptop, desktop, mobile device support	
S/MIME support	
Shared mailbox S/MIME support	
Native Exchange Onlone support	
Server (application) support	
Webserver SNI support	
REST API support	
SCEP support	
ACME support	
Automated S/MIME configuration of Outlook	
CKMS Operating System	Ubuntu 22.04 LTS
High Availability Db	MySQL 8
Cloud & Hypervisor compatible with	VMware, HyperV, Azure, AWS, Google
Production, pre-production, acceptance environment default part of the license	
Air gapped environment support	
Average new firmware upgrade time (incl HA)	5 minutes
Supported Community Size	Up to hundreds of millions
Multi-tenant	
Management authorization roles	
Self-Service portal	
Internal private CA	
Load Balancer support	
3rd party private CA support	MS ADCS, EJBCA
Partnered Certificate Service Providers & certificate vendors	DigiCert • GlobalSign • Sectigo
Revocation and CDP support	
CSR certificate key length	2048 - 8192 bit RSA • Up to 521 bit ECC Ready
IDP supported modules	Active Directory / LDAP • Azure Active Directory • Internal MySQL Db • MySQL • RADIUS
Certificate publication	Intune, Mobile Iron, Workspace ONE UEM
MDM support	
HSM support	
TPM 2.0 support	
Key attestation support	
Certificate and Key roll-over (S/MIME, etc)	
Reporting and dashboard	
Logfile Syslog/SIEM support	
Secret encryption	AES 256
Automated (encrypted) backups	AES 256
Automated security updates	Hourly
Device identification	
Stand-alone LDAP S/MIME address book	Up to 50.000.000 Users
Certificate discovery	Dedicated Virtual Appliance Solution
Feature customization	Often within 6-8 weeks at customer request
Free Proof of Concept support	
Public status	Privately Owned, 100% Dutch
Standard support	24/7 in English, French, Dutch, German
Visitor address	Maanlander 47, 3824MN, Amersfoort, NL

sales@keytalk.com • www.keytalk.com