whitepaper 2015

Beyond PKI

Manage your PKI more efficiently with KeyTalk's automated certificates

Summary

This whitepaper describes how Public Key Infrastructure (PKI) overhead can be significantly reduced for your internal network. It will also inform you how to move away from the traditional username and password authentication to the more efficient 2-Factor or Multi-Factor Authentication using KeyTalk's distribution platform of short-lived X.509 certificates.

With our KeyTalk solutions you will cut costs, leverage your IT security and address upcoming regulatory compliance issues.

More information

Should you wish more technical information regarding KeyTalk solutions, please contact us at:

info@keytalk.com

For commercial information, please send your inquiry to:

sales@keytalk.com

Public Key Infrastructures (PKI's)

A Managed PKI from a well-known Certificate Service Provider or an on premises PKI from an open-source based project tend to be a time consuming, expensive and administrative challenge. PKI management demands valuable time of your IT department as your network ecosystem evolves due to employee changes, changing suppliers, growing customers, more user devices, larger server environments and multiple domains.

The challenges start as a optimistic dream wherein the initial certificate enrollment is well addressed in a proper project manner with a defined timeline. But then the project is delivered and the need for reissuing certificates start. Followed by revocation and certificate renewal. Frantic calls to your internal support desk come in from end-users who are unclear how to install certificates on their own devices. Alternatively, a security bug such as "Heartbleed" is exposed and expedited thereby requiring certificate revocation and replacement on all your servers after proper patching.

Despite these important facts of PKI, virtually all companies make use of PKI in one form or another:

1) It's been proven to be safe as the X.509 standard has never been successfully hacked.
2) It's a de facto standard since 1988. All computer network environments can deal with the X.509 standard on which PKI is built.
3) It has many applications.
4) It supports most IT security based compliance issues.

Classic PKI's have a large number of applications such as S/MIME email encryption, server identification, web application user identification authentication & authorization, IoT device identification, Network Access Control, digital document signing, 2 way SSL authenticated data-in-motion encryption over TLS, user authentication for VPNs, enterprise server application Single Sign-On, etc.

Despite a number of technical and operational drawbacks, PKI is here to stay. It's safe to say that anything that helps to alleviate these classic PKI downsides is met with open arms in the worlds of IT and Cyber Security.

Beyond PKI

In 2003, KeyTalk already saw the potential of X.509 and how it could positively leverage the end-user experience and assist in the future of Cyber Security. As a result of our advanced technology being globally patented in 2006, managing the potential for your PKI has become much more manageable and easier to implement.

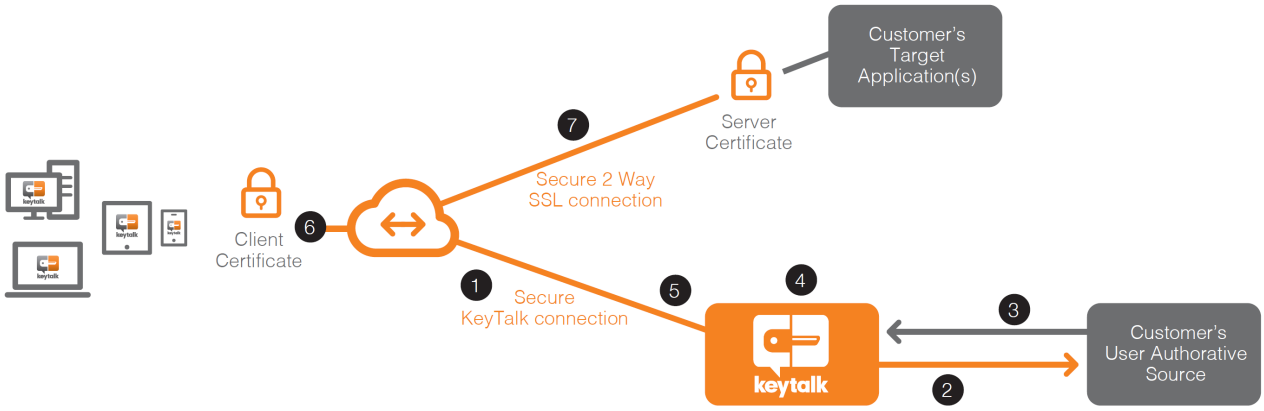
KeyTalk addresses the downsides of classic PKI implementations by taking the innovative approach of offering short-lived certificates for closed user (device) and server group communities. It also offers the secure and automated distribution and de-installation of client and server X.509 certificates. Not exclusively in your domain like Microsoft already denables, but beyond your domain(s) for heterogeneous device and server environments.

By introducing certificates with a life span shorter than the need to update revocation pointers (CRL & OCSP), KeyTalk takes away the need for revocation pointers. This alleviates your IT department from the burden of certificate administration. Certificates might be valid for anything ranging from a few seconds up to a day, or even one month, depending on your company policy.

One of the primary pillars in a PKI is your Registration Authority.
By connecting your existing authorative IAM system(s), such as Active Directory or RADIUS based tokens, to your PKI system, you can easily automate the Registration Authority without a need to replicate your IAM data. After all, you already trust your IAM systems.

Unfortunately, PKI and a positive end-user experience are rarely found in the same sentence. Requesting and installing certificates is a burden.

Trusting a Root and sub-CA raise more questions than give answers. Simply put, most end-users neither understand PKI nor do they want or need to. Consequently, KeyTalk makes the process automated and seamless by requiring a small app or SDK that efficiently takes care of all the certificate enrollment aspects.



1) *The KeyTalk client/SDK triggers the authentication to obtain a certificate in a secure manner to the KeyTalk (virtual) appliance*
2) *The KeyTalk appliance verifies the authentication credentials against the customer's authorative source*
3) *The authorative source approves (or denies) the authentication*
4) *KeyTalk verifies the hardware fingerprint of the device and creates the certificate and key-pair*
5) *From the KeyTalk (virtual) appliance the certificate and key-pair are sent securely to the client device, such as the IP-camera or smartphone/laptop*
6) *KeyTalk's client/SDK installs the obtained certificate and key-pair, and uninstalls the old one.*
7) *The connection from the device to the target server environment is secured during initial handshake or when renegotiating the handshake using a proper X.509 certificate and unique key-pair*

Despite PKI offering a range of applications for issued certificates, most companies who have deployed PKI tell us that they only use their PKI for a few applications as enabled by PKI, such as:

- Mutually authenticated data-in-motion encryption
- secure server application access
- end-user device recognition
- federated identity
- convenient end-user Single Sign-On and occasionally
- role-based-access control

If data-at-rest encryption isn't needed, then KeyTalk's automated short lived certificate life cycle management could benefit your company. It will not only alleviate the PKI burdens of your IT and Compliance departments, it will go beyond PKI. Providing significantly leveraged network access control on strong authentication.

Patented certificate request and distribution

Most Communications Service Providers (CSP) will offer to create a Certificate Signing Request (CSR) for your company due to its inherent complexity. Furthermore, Internet of Things devices are often incapable of even creating a CSR.

In 2006, KeyTalk patented its secure method to create a CSR on the server side and use a secure channel over non-secure network connections such as the Internet. This would facilitate and deliver the resulting X.509 certificate with corresponding strong encryption key-pair to a target device.

The result is an incomparably easy to use method to deliver X.509 certificates. These certificates can include key-pairs anytime, anywhere for any length of time through default port 80. This prevents potential firewall issues and ensures security due to using HTTP encapsulation encryption.

A glance at Registration Authority

A Registration Authority (RA) is required in PKI. Without it you will not be able to sufficiently verify if a request of a certificate is valid for the right device/server/user by a valid requesting source.

KeyTalk's PKI engine connects securely to your existing IAM (Indentity Access Management) system(s) such as: Microsoft Active Directory, LDAP, RADIUS, MySQL etc.

With several IAM frameworks no longer being in the central network, and compliance requiring inter-network traffic being encrypted, the connection from KeyTalk to your IAM is secured using defacto standards. Active Directory and LDAP are secured using LDAPS and RADIUS based connections use EAP to ensure proper data encryption.

By ensuring that data doesn't need to be replicated, the Admin doesn't introduce yet another to be managed data-source. How does KeyTalk do that? For example, we do a live lookup using a BIND of LDAPS.

Since your IAM is generally is up to date, KeyTalk addresses one of the chronic problems found in a classic PKI; namely keeping the credentials in the issued certificate up to date. How? When a short-lived certificate request has been positively authenticated based on verified received authentication credentials, these same credentials are used to query the Active Directory attributes. These attributes can be mapped to any X.509 certificate field, overwriting default settings, making it part of the KeyTalk generated CSR. This includes certificate lifetime, subject alternative name values and (extended) Key Usage.

Should KeyTalk not offer a native connector to your IAM system(s), we offer a backend API allowing you to define your own, or ask us through our partners to develop and integrate a connector based on your specifications.

Adding Multi Factor Authentication

Phishing (identity theft) is a widespread and growing problem. Passwords are no longer sufficient to protect accounts.
Two factor (2FA) and multi-factor authentication (MFA) have become a necessity.

KeyTalk integrates with most 2FA/MFA solutions as long as we can interface with them. This facilitates a better user experience and improved usability since tokens are only needed once or twice per day.

Most companies seek integrated solutions which not only work with their users, but also with their servers and Internet of Things (IoT) devices. Tokens for these customers regularly do not suffice because an OTP generator often can not be used on a server or unmanned IoT device. In short, you clearly don't want to introduce a weak authentication link in your total network eco-system.

KeyTalk introduces a strong authentication factor on top of any IAM system you have in place. The KeyTalk factor looks at trusted device characteristics, whereby measured components go beyond traditional browser based meta-data. While your MAC address might be sufficient to use despite its vulnerability to spoofing, KeyTalk offers a wide variety of different components depending on the target device operating system. These include the BIOS serial number, total memory, CPU InstanceID, OpenUDID, onboard sensor availability, SSH key and SIM card number and many more. Most importantly, KeyTalk does not require the admin to use all the components we make available. The admin can mix and match. If you don't want to use a MAC address, simply remove it. Would you like the total memory to be used twice in the hardware identification hash calculation in the 3rd and 7th place? Configure it like that. This means that even a manufacturer such as KeyTalk won't know what you are using.

Though hardware identification is offered as an added multi factor layer, you can even choose to use it as a primary factor. This is especially useful

for servers and IoT devices where you may not want to use preprogrammed static usernames and passwords.

Using your own Certificate Authority (or not)

Most CSPs offer you little choice with regards to choosing a Certificate Authority (CA). At KeyTalk we offer you a simple choice: Our way or your way.

Most of our customers already have a CA or even multiple copies of the CA across multiple domains. Replacing an existing CA is rarely a good idea, if only because you do not want to configure your network with a new primary trust. In these circumstances, you can set your own CA as the root under which the primary and signing CA of KeyTalk are generated on the KeyTalk virtual appliance. Or you can simply import your entire preferred CA into the KeyTalk product. The root and primary CA private keys are of course kept offline.

Alternatively, you can easily setup your own CA using SHA2 and up to 4096 bit RSA keys. As a minimum a primary and a signing CA are directly used on KeyTalk. It's a short and simple configuration which results in KeyTalk generating the required CA-tree with sufficient entropy for the signing keys.

This flexibility also allows you to take into account any key ceremony requirements which might be needed from with regards to compliance.

Imagine your CA needs to be replaced and you've got a large community that needs certificates under your new CA. With the KeyTalk solution, you create your new CA, enroll the new digitally signed KeyTalk trust configuration to the clients and the next certificate installed on the user device is under your new CA.

Hardware Security Modules (HSM)

In most cases, PKI systems are well protected in customer network environments. But most customers do not have the resources to invest in an Hardware Security Module (HSM) cluster to protect their private keys.

KeyTalk does not require the use of an HSM. By default, we store the certificate signing key directly onto the KeyTalk server. For most companies this is acceptable since internal procedures and backup processes will safeguard the access to the signing keys. Within your compliance scope, this choice fits perfectly.

KeyTalk also caters to those companies who do have the resources and have implemented their own HSM. Given the fact that KeyTalk runs on a hardened OpenBSD OS and integrates LibreSSL for its default crypto, PKCS#11 is fully supported. But not all HSM manufacturers actually supply libs to interface with their specific HSM. To address this issue, KeyTalk comes with a secure HSM proxy based on Linux, which overcomes the lack of support by HSM manufacturers on OpenBSD.

Multi-tenant scalability

Once you automatically start issuing X.509 certificates to your users and server community, scalability becomes a must-have feature. Particularly, when you are issuing on average 365 or more X.509 certificates per target client/server per year.

Multi tenancy is also a must have. Since most communities make use of multiple IAM targets from a security perspective, you may wish to service different customers or departments with different default certificate settings. Our partners also may offer KeyTalk as a Cloud service thus requiring it to be multi-tenant.

Scalability is always determined by the weakest link. For example the KeyTalk cluster might be able to issue 1000 certificates per second. But if your IAM system can only process 100 requests per second, then there are other components which first need to be scaled by you or your system integrator.

The KeyTalk appliances are available physically and virtually. The choice for OpenBSD as our primary OS defines the compatibility with the hypervisor. VMWare supports OpenBSD. Whereas at the time of writing HyperV does not fully support OpenBSD.

KeyTalk virtual appliances are provided free of charge, allowing you to scale indefinitely using a Cache Array Routing (CARP) mechanism. Whether you need to cater to a community of 10 persons or 10 million connected cars. KeyTalk scales well.

Since CARP on VMWare brings its own security challenges, such as a need to enable promiscuous mode, the KeyTalk cluster is advised to run in its own VLAN.

For larger automated environments whereby scaling needs to happen more dynamic, KeyTalk can make other scalability mechanisms available. These mechanisms also overcome the need for promiscuous mode.

Though KeyTalk supports built-in high availability, load balancing still requires an external solution in order to create an active-active HA environment.

X.509 SSO: Interoperability at its best

User experience is key.

All known operating systems support X.509 for secure 2-way authenticated SSL over TLS. And though many enterprise applications support the X.509

client certificate for single sign-on purposes, there are also many who do not such as the increasingly popular (Cloud) network environments.

When the market demanded a solution to overcome the limitations of target server applications which didn't supporting client certificates for a secure single sign-on experience, KeyTalk developed its own Application Interoperability Layer (AIL).

This AIL is a secure redundant proxy based on a Linux OS that requires client certificates from a specific CA to connect to it over TLS. Depending on the target url/ip being addressed, it will terminate the TLS connection or let it pass to the target server application.

When it terminates due to the target application not supporting client certificates, it will convert the verified client certificate credentials into something the target application understands and expects. This might be a SAML token or a username/password or even something else. It all depends on the target application.
It may also be used for username mapping whereby the common name value in your certificate is, for example, your AD or RADIUS username but the target application may expect something totally different.

A secure connection is established over TLS between the AIL and the target application. The user experiences a seamless and simple single sign-on process.

Digital threat mitigation with KeyTalk

Digital threats are increasingly present not only in technical but mainstream media as well. Rather than users being the target of phishing attacks, the news outlets are writing malicious parties as well as government agencies using advanced techniques to eavesdrop on our data-in-motion and infiltrate our corporate networks.

One of the most commonly published digital threats are known as Man-in-the-Middle (MitM). Though most 2-factor authentication solutions provide excellent strong authentication, they don't protects against MitM using Wifi, wired or cell-phone based connectivity.

Though new standards such as HSTS are gradually being embraced, PKI is the only reliable method of preventing the full range of MitM threats to your network.
As is generally the case with IT security, the assumption should be made that your PKI or network is properly configured and is not compromised.

KeyTalk has been designed from the ground up to protect against MitM and is periodically tested by independent ethical hacker teams to prove our security claims.

Furthermore, KeyTalk solutions enable protection for phishing and anonymous brute force threats. Please refer to our website for further security information.

KeyTalk solutions do not protect against are threats such as Man-in-the-browser and compromised networks/client devices. KeyTalk works closely together with parties who offer solutions that typically address these specific threats.

Compliance

It's almost impossible to address the wide array of compliance regulation issues that exist in today's digital and offline world. It's safe to say that given the plethora of digital security threats that KeyTalk solutions mitigate we address your companies compliance needs.

In 2016, the European Union Data Protection Reform will take effect in 2016 and will come into full force in 2017. In summary, violations of the Data Protection Reform Act can result in fines starting at EUR 450.000. This could translate into 2-10% of your company's group yearly revenue in fines when privacy data is leaked. After all, your network infrastructure is meant to reliably protect privacy sensitive data.

Companies will need to address data leakage, especially when it comes to private, personal and sensitive information. This information doesn't just relate to a persons name or social security number. Recent court rulings have proven that someone's location, such as a registered by car tracking software or even your smartphones location tracking, will fall under the Data Protection Reform.

Hiding behind the fact that you implemented a firewall and/or a token will not be enough. Most professionals agree that there are far more things you can do to address with today's available (security) technology and products.

Customer Testimonials

The KeyTalk product development started in 2003. Its initial production ready development cycle lasted until 2005 when the first pilot was done with a major Dutch bank. In 2006 our first production customer Oce/Canon was enrolled. This was followed by The Council of the European Union, Marel (formerly known as Marel Food Systems), ForFarmers and several others whose names we cannot disclose.

***Philippe de Penaranda, security advisor Council of the European Union*:**

“Secure yet convenient access to SAP was a must-have for us. Introducing KeyTalk into our network environment made this possible, and a lot more.”

Marcel Janssen, ICT manager Océ:

"Our return on investment was realized within 6 months’ time. We believe this to be an excellent ROI. Using the KeyTalk solution and combining it with the F5 webvpn platform, our employees can make use of their existing identity and authentication credentials to obtain their digital certificate which provides them access to the required remote applications and network. This certificate is stored directly onto their mobile device and is valid for a predetermined period of time.

Maintenance and support wise, both our user community and administrators highly appreciate the KeyTalk solution. On average our internal support receives 1 support call per quarter based on several thousand end-users. Maintenance wise we spend less than 10 hours per year on the overall solution. Prior to deploying the solution we had both a leading token and the KeyTalk solution evaluated by our end-users. On average 95% of our users accepted the KeyTalk solution within the first month, whereas the token solution was only accepted by 60% of the users within the initial 3 months.

Conclusion

The KeyTalk solution addresses problems companies struggle with when it comes to:

- PKI
- Strong Authentication
- Network Admin workload and
- the balance between reliable security and a positive user experience

Let KeyTalk put an end to your PKI struggles.

More information

Should you wish more technical information regarding KeyTalk solutions, please contact us at:

info@keytalk.com

For commercial information, please send your inquiry to:

sales@keytalk.com

Contact us at
welcome@keytalk.com

keytalk.com