Windows app manual

Contents

1. Introduction 2
2. Installation 2
   2.1. Guided installation 2
   2.2 Silent installation Windows end-user device 4
   2.3 Silent installation Windows Servers 4
3. Configuration 5
4. Requesting a user certificate (and crypto key-pair) 6
5. Reporting a problem : logfiles 6
6. Requesting and auto-renewing an IIS and/or Websphere certificate 7
7. Auto configuring an S/MIME LDAP secure email address book for Outlook 8
8. Auto configuring S/MIME email signing and encryption for Outlook 8
9. Command line KeyTalk client 9
10. Remote Desktop / Citrix environment KeyTalk client support 9
11. TPM 2.0 based virtual smartcard support 10
12. Renewal Windows Scheduled Tasks explained 10
13. KeyTalk support and contact details 11

Company	KeyTalk 1 BV
Author	MR van der Sman
Creation date	9 August 2015
Last updated	03 June 2023
Product	KeyTalk Windows agent
Data classification	Public
Software version	7.2.0
Manual version	7.2.0.1

1. Introduction

The KeyTalk app for Windows is used to as seamlessly as possible deploy X.509 certificates to Windows laptops, PCs, and servers, and optionally auto configure for Outlook a KeyTalk serverside configured external LDAP address book, as well as the email encryption certificate for outgoing emails, and the optional textual signature/disclaimer.

These X.509 certificates are mostly used to:

- Enable email encryption and decryption
- Enable email signing to combat Business Email Compromise
- Securely authenticate to Wifi, VPN and server applications using 802.1x
- Digitally sign documents
- Enable TLS on (web)servers

The KeyTalk agent for windows comes in 2 flavors:

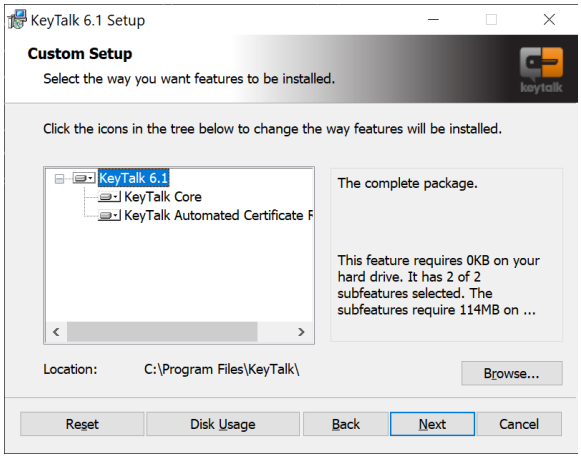
1) The generic enterprise KeyTalk agent: it supports various methods of authentication, supports the use of various certificate templates, and is compatible with Windows 7/10 and the Windows server range.
2) The Secure Email Service KeyTalk agent: It's a simplified version of the KeyTalk enterprise agent, focused solely on issuing S/MIME certificates using a One Time Password methodology. This version does not support multiple certificate templates and does not support the Windows server range

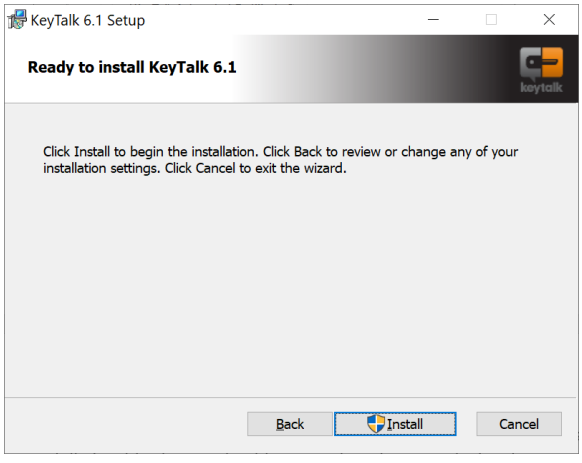
2. Installation

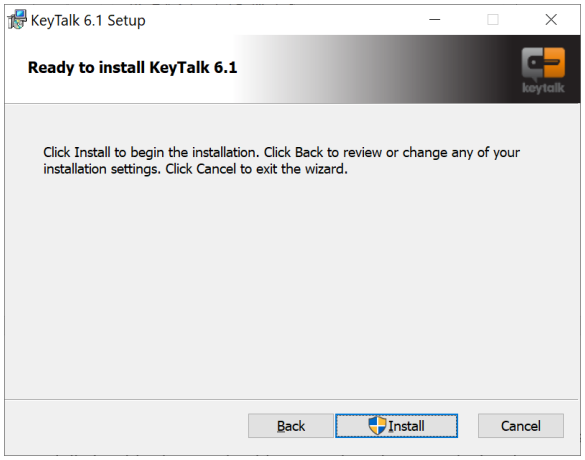
To install the KeyTalk app for Windows, administrator permissions are required.
Using the app only requires regular user permissions.
Note: depending on whether you are installing the Secure Email Agent or the KeyTalk Enterprise agent, the installation screens may differ from those documented below.
For use of S/MIME automated Outlook configuration ensure your KeyTalk agent matches with the X64 (64 bit) or X86 (32 bit) version of Outlook.

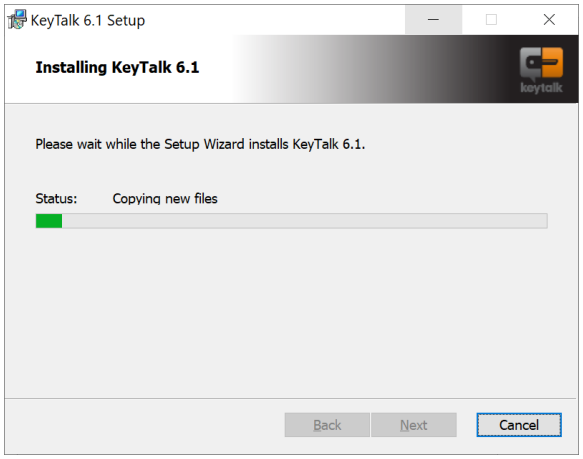
2.1. Guided installation

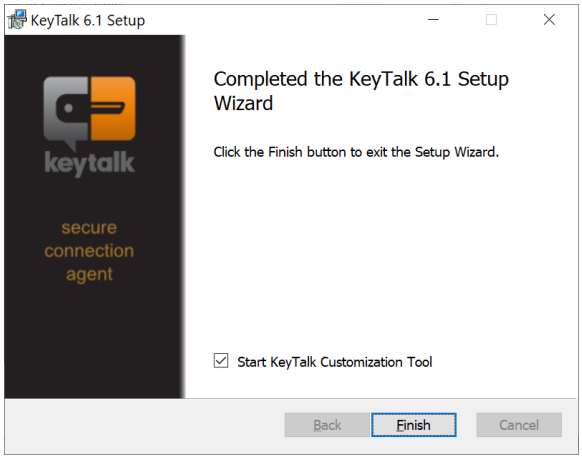
Install the KeyTalk app as found here: https://www.keytalk.com/download#clients

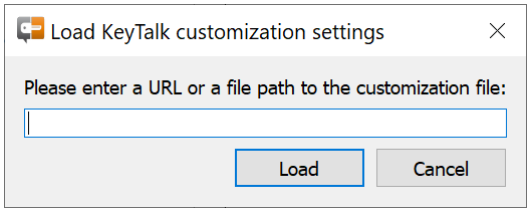


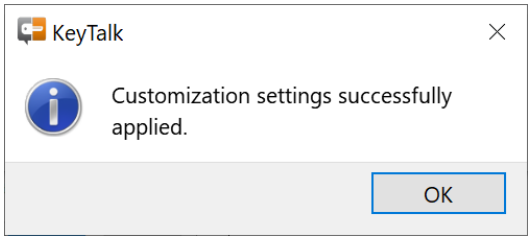




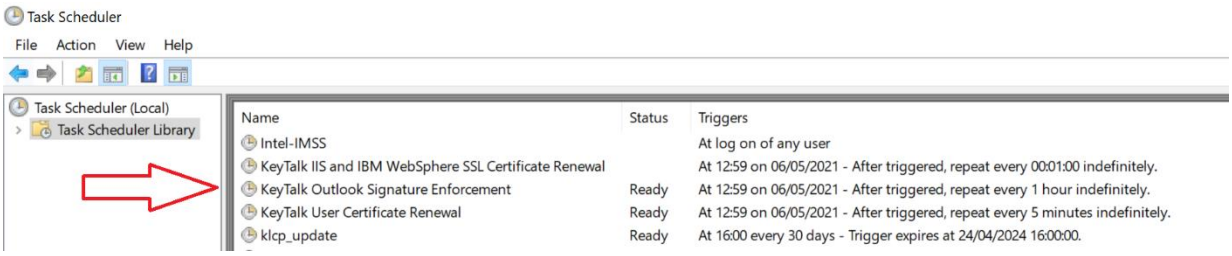








The KeyTalk agents adds tasks to the Windows Task Scheduler regularly checks if the installed certificates are about to expire, have been revoked, or have expired, in which case the KeyTalk app will be invoked for renewal.



When invoked the KeyTalk agent will try to renew in the background thus not bothering the user, but if an active interaction with the user is required the KeyTalk agent will pop-up.

2.2 Silent installation Windows end-user device

Most administrators will prefer a silent installation to multiple laptops/desktops
With the KeyTalk app for Windows being an MSI the administrator can easily repackage his own installer, or the administrator can use the following command:

```
cscript /nologo MsiSilentInstall.vbs path\\to\\msi [ full-path\\to\\rccd [rccd-proxy-user rccd-proxy-password] ]

Example: msiexec /i KeyTalk.msi /qn RCCDPATH=https://downloads.keytalk.com/test.rccd
```

2.3 Silent installation Windows Servers

Most administrators will prefer a silent installation to multiple servers, whereby the server configuration task (task.ini) is also included in the silent installation.

The below is an example on the task.ini file to configure a target Windows server with IIS using a default IIS binding IP (0.0.0.0):

```
ConfigVersion = "2.0";
TaskList = (
 {
  Name = "Task_Server";
  TaskType = "Regular Task";
  UseIISBinding = false;
  UseWebSphereBinding = false;
  KeyTalkProvider = "MyCompany";
  KeyTalkService = "Server_Internal-KeyTalkCA";
  KeyTalkUser = "__KT_HOST_FQDN__";
  KeyTalkPassword = "";
  CertificateStore = "My";
  CertApproverEmail = "";
  TrackComputerName = "Do not track";
  HttpsBindingIp = "0.0.0.0";
  HttpsBindingDomain = "";
  HttpsBindingPort = 443;
  WebSphereKeyDbTypeParam = "pkcs12";
  WebSphereKeyDbPath = "";
  WebSphereKeyDbPwd = "";
  WebSphereHttpServerPath = "";
  WebSphereCertLabel = "";
  ScriptLogFilePath = "C:\\Users\\test \\AppData\\Local\\Temp\\keytalk_task_Task.log";
  EmailReporting = false;
 } );
```

NOTE!: *"__KT_HOST_FQDN__" is a parameter value unique to KeyTalk agent 7.2.0 and automatically selects the servername as the username in the task.ini once its opened and resaved.*

With the KeyTalk app for Windows being an MSI the administrator can easily repackage his own installer, or the administrator can use the following command:

```
cscript /nologo MsiSilentInstall.vbs \path\to\msi \path\to\rccd  --tasks-ini \path\to\tasks.ini
```

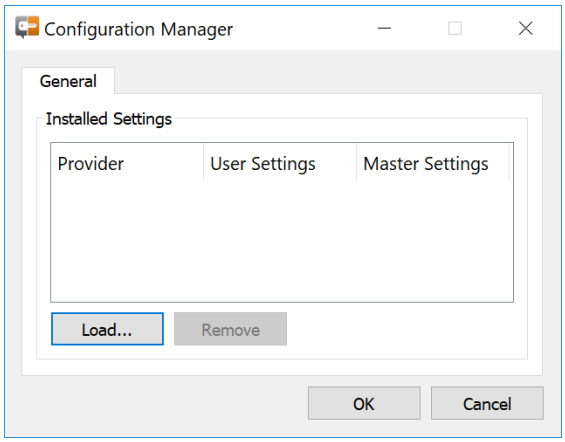
3. Configuration

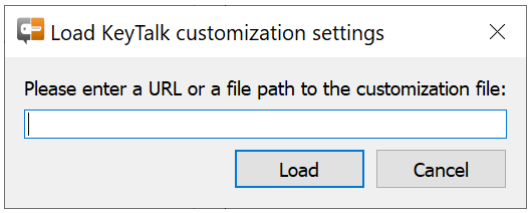
Each KeyTalk app requires a configuration file. Without it the KeyTalk app doesn't know where to contact the KeyTalk virtual appliance to request a certificate.

Additionally, the configuration file enables the KeyTalk app to set the corporate KeyTalk Certificate Authority as trusted on the Windows laptop/PC.

The needed configuration file is a Real Client Configuration Data file, or RCCD. It only contains public information so can be distributed on the open internet when need be.
Most companies will distribute it either by means of a url or by email.

To import this configuration file into the KeyTalk app, the app will automatically ask for it when a configuration file is missing.
Or you can manually load it by starting the "KeyTalk Configuration Manager" as found under installed programs.



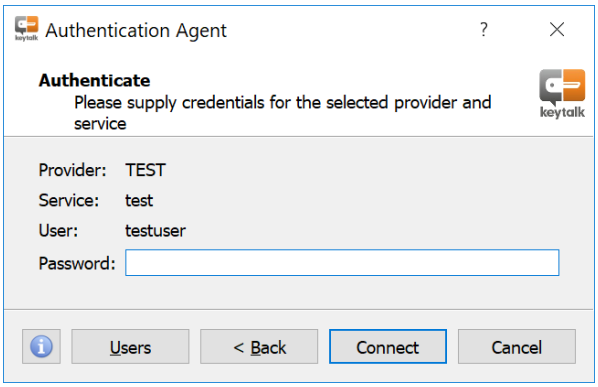


The actual config settings can be found under: *\AppData\Roaming\KeyTalk\user.ini*

4. Requesting a user certificate (and crypto key-pair)

Once the configuration file has been loaded, the KeyTalk app will be able to fetch a certificate for the user (or the server)

Depending on the KeyTalk server administrator enforced configuration settings, the user may be requested to type his/her corporate authentication credentials, such as username/password or token based One Time Password:



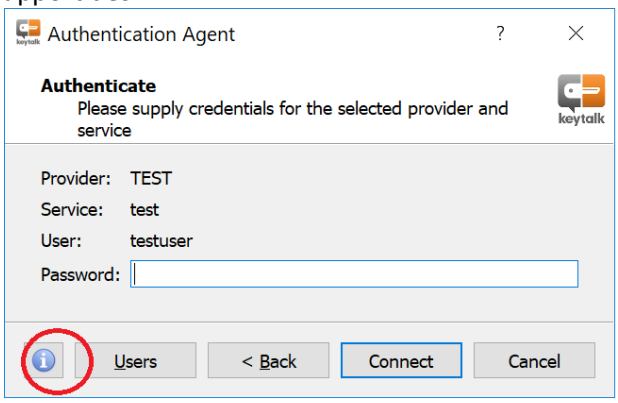
Alternatively, no username/password or other credentials might be asked, as Kerberos based silent authentication is also supported. When using Kerberos, a username/password will only be requested if the Kerberos token is found not be valid or usable.

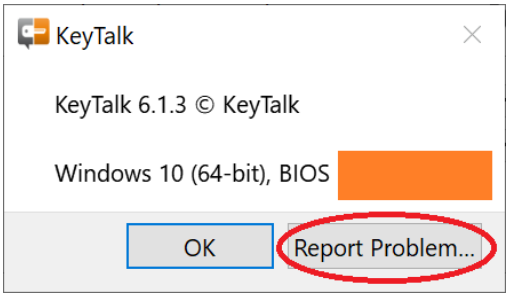
A message will appear when a certificate was successfully obtained and automatically installed.

Should you wish to inspect the installed certificate, open CMD or Powershell and type: certmgr or mmc

5. Reporting a problem : logfiles

The KeyTalk app keeps a local logfile for trouble shooting purposes.
Should a user encounter any issues, the user can generate a problem report and send it by email to his support desk:





Users and support staff can easily open the generated Problem Report, by renaming the created DAT file to ZIP and opening it. The container contains several relevant logfiles, whereby the most notable log is the ktclient.log file.

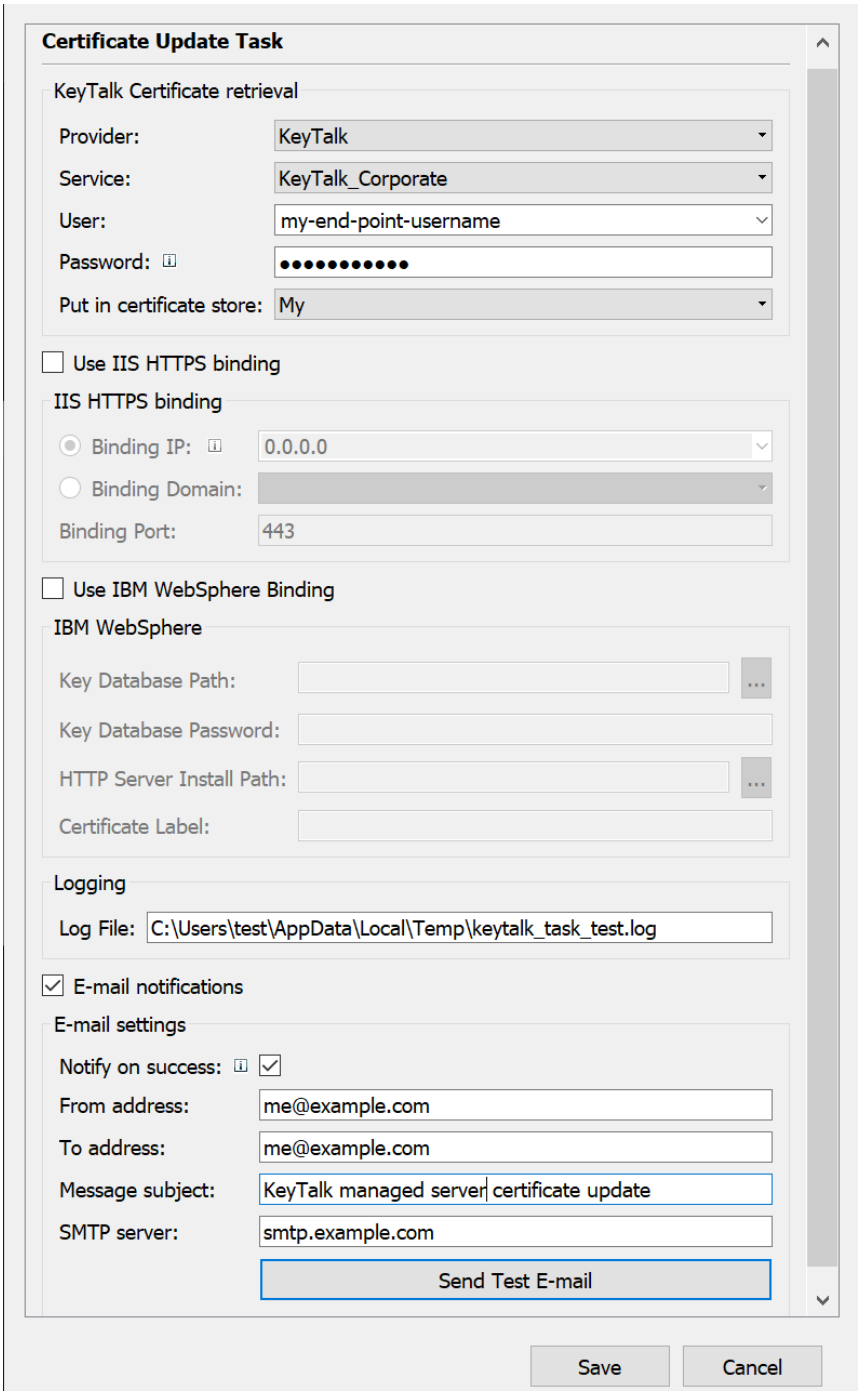
This logfile can also be directly found under the current user's \AppData\Roaming\KeyTalk

6. Requesting and auto-renewing an IIS and/or Websphere certificate

Following the KeyTalk app installation process and configuration, an administrator can finalize the configuration to automatically fetch, renew, and bind certificates to IIS or Websphere HTTP.

- The KeyTalk app/Configuration Manager must be run with **administrator** rights
- The IIS server must be configured for SSL/TLS
- IIS version must be minimally 7.5
- The Windows server must be minimally 2012R2
- The KeyTalk virtual appliance SERVICE must be set to issue server certificate (Extended Key Usage = Server Auth)

From the KeyTalk Configuration Manager, create a certificate task as administrator of the Windows server:



To mass deploy your server certificate management template you can use:

```
> cscript /nologo MsiSilentInstall.vbs "c:\KeyTalkClient-5.X.X.msi"
"c:\MyProvider.rccd" --tasks-ini "C:\tasks.ini"
```

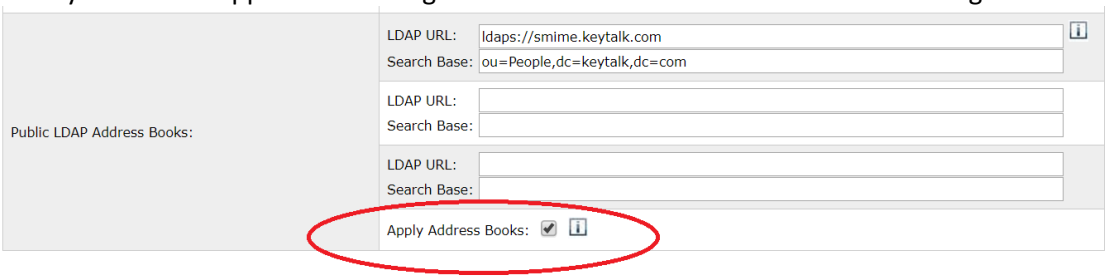
In order to support SNI hosts, 1 task needs to be created per SNI host.

7. Auto configuring an S/MIME LDAP secure email address book for Outlook

When the KeyTalk virtual appliance has been configured to configure client side an LDAP address book, containing email address public keys to support S/MIME email encryption, the KeyTalk client will facilitate this configuration provided local user right allow for this.

The automated configuration will only happen when:

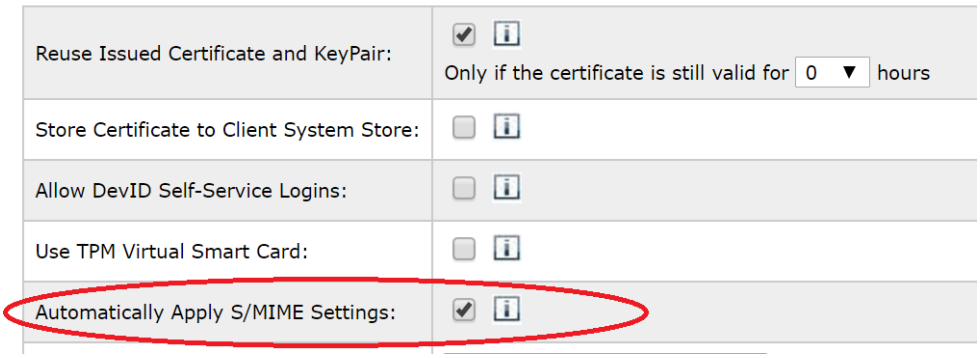
a) The KeyTalk client 32/64 bit version matches the bit version of the installed Outlook
b) Outlook is set as the default mail client
c) The KeyTalk virtual appliance is configured to enforce the LDAP address book configuration



8. Auto configuring S/MIME email signing and encryption for Outlook

When the KeyTalk virtual appliance has been configured to configure client side email encryption and signing for Outlook, the Windows KeyTalk client will attempt to do so:

Certificate Settings



Clientside the Outlook default email address is expected to the main email address the certificate is issued to.
If the main email address does not match with the S/MIME certificate's email address, a best match email address is configured Outlook side for the S/MIME email certificate as obtained by the KeyTalk client.

The KeyTalk client will enforce SHA256 as the hashing algo and set AES 256 as the encryption algo. Additionally it will set email signing to always on. Email encryption is not set automatically.

Note: The KeyTalk client for Windows will not publish the configured certificate to GAL. Reason being that publish to GAL only exists in single email configurations on Outlook, and AD syncing periodically with Exchange for GAL purposes, whereby KeyTalk virtual appliance already publishes the certificate to AD and to a configured LDAP Address book, such as the KeyTalk LDAP key server/Address book

9. Command line KeyTalk client

Hardcore command line users, or those who wish to script their processes, can also use the KeyTalk client from the command line.

The command prompt client can be found in the KeyTalk program installation directory, usually: "C:\Program Files\KeyTalk\ReseptConsoleClient.exe"

Resept is an ode and reference to the 2003 original internal project name for the product now known as KeyTalk.

To see all possible commands, type: ***reseptconsoleclient –help***

A sample command could be:
reseptconsoleclient --user test --password test --save-pfx
In this example we assume a single KeyTalk service RCCD config file was loaded into the KeyTalk client, and as a result the reseptconsoleclient will automatically assume that the only available KeyTalk provider and only available service needs to be addresses, using the username test and password test with the certificate output in PFX format (and a separate private-key password file).
The saved PFX and passwordfile can be found in: \AppData\Local\Temp\keytalk.pfx and \Local\Temp\keytalk.pfx.pass

A sample command could also be:
reseptconsoleclient --provider PROVIDERNAME --service SERVICENAME --user test --password test --save-pfx
Similar to the first example, in this case a more elaborate KeyTalk configuration likely applies, whereby multiple KeyTalk providers (ie KeyTalk clusters) are available to choose from, and multiple KeyTalk services are available to choose from, therefor requiring the KeyTalk provider and service to be specified.

When instead of a PFX a PEM file is preferred, use –save-pfx , AND change the user.ini (see chapter 3) to include:
CertFormat="PEM";

NOTE: Kerberos based authentication is currently reserved only for GUI based client use.

10. Remote Desktop / Citrix environment KeyTalk client support

Remote Desktop and Citrix environments are hardly ever single server based.

When deploying a KeyTalk client for a user, the KeyTalk RCCD configuration file needs to be available on every server instance the cluster.

The KeyTalk client supports a master config file which can be embedded in any KeyTalk RCCD file upon creation in the KeyTalk virtual appliance.

This config file is installed in the /Users/Public and will be automatically copied to a User, when a KeyTalk config file is missing, or is deemed corrupt.

See chapter 14.3 in the KeyTalk virtual appliance manual for more information on how to include the master config.

11. TPM 2.0 based virtual smartcard support

The KeyTalk client for Windows also supports TPM 2.0 based virtual smartcards.

As a result a private key is generated on the TPM, based on the Certificate Signing Request meta data as defined in the KeyTalk service, provided that TPM Virtual Smart Card support is selected.

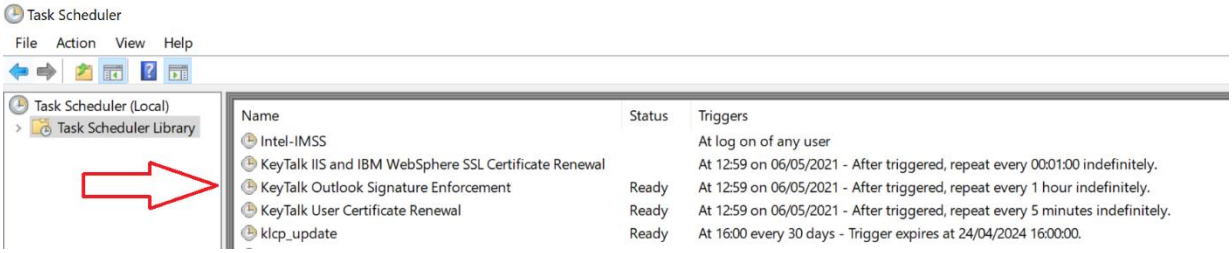
When the client sends back the CSR to the KeyTalk virtual appliance to have it signed, the meta data in the CSR is verified against the enforce KeyTalk service configured minimal certificate meta data. If it doesn't match the certificate will not be issued. This feature has been implemented to prevent skilled users from manipulating the data generated by the KeyTalk client.

The KeyTalk client for windows does not activate and configure a virtual smart card as of yet. It currently assumes the Admin has already done so.

NOTE: Key roll over is not supported when using TPM based virtual smart cards.

12. Renewal Windows Scheduled Tasks explained

Upon installing the KeyTalk client, two scheduled tasks will be added to the Windows instance, aiding in the monitoring of the installed certificate validity status, and when it should be renewed.



KeyTalk IIS and IBM WebSphere SSL Certificate Renewal
This script runs checks on all the tasks as setup in the KeyTalk Configuration Manager.
By default the script runs every single minute, checking whether the certificates related to the task are still valid.
When a new/renewed certificate is required it automatically requests this certificate from the KeyTalk server using the KeyTalk client, and stores it to the relevant certificate store.
It also updates the IIS binding to the new certificate if the task requires it.

KeyTalk User Certificate Renewal
This script checks with the KeyTalk client if the certificate for the latest provider/service is still valid. By default the script runs every 5 minutes. If a new/renewed certificate is required it attempts to quietly refresh using Kerberos if the Service allows this. Otherwise it will open the KeyTalk client for the user to authenticate.

KeyTalk Update Outlook Signature Enforcement
This script checks with the KeyTalk client if textual email signature/disclaimer needs to be updated. The textual signature/disclaimer is fetched from the KeyTalk server only if a valid S/MIME belonging to the email address as configured in Windows Outlook is present.

13. KeyTalk support and contact details

KeyTalk provides third line support to its commercial partners.

For 1st and 2nd line support kindly contact your IT department or your KeyTalk supplier, and include a description of your problem together with a generated client Problem Report.

Should you feel there is a need to directly contact KeyTalk for technical support or technical questions, kindly raise a ticket using: https://support.keytalk.com
or email us at: support@keytalk.com

Should you have commercial related questions, kindly email us at: sales@keytalk.com

Our office details:

Company name:	KeyTalk I BV
Dutch Chamber of Commerce registration:	59072555
VAT number:	NL853305766B01
KeyTalk HQ address:	Maanlander 47 3824MN Amersfoort The Netherlands
KeyTalk billing:	Keulsekade 218 3534AC Utrecht The Netherlands