# KeyTalk Firmware 4.2

### **Administrator Appliance Manual:**

Installation and settings

KeyTalk Documentation



This document is propriety of KeyTalk BV. This is a controlled document; it may not be copied and nothing in it may be changed without knowledge and consent of KeyTalk BV.

© Copyright KeyTalk BV. All rights reserved.

The information in this document is subject to change without notice. No part of this document may be reproduced, stored or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of KeyTalk BV.

KeyTalk BV assumes no liability for any damages incurred, directly or indirectly, from any errors, omissions or discrepancies between the software and the information contained in this document.

KeyTalk is a registered trademark and the KeyTalk logo is a trademark of KeyTalk BV.

Document name: KeyTalk Client 4.2\_Appliance Manual

Version: 4.202 Date: 26-Jul-13



### Document control

Document information	
Author	Michael van der Sman
Owner	KeyTalk BV
Document Version	4.202
Document status	Final

Revision # & Date	Summary of Changes	
4.002 22Jun11	Initial release	
4.003 13Jul11	Added chapter on LCD display, updated Remote Exit chapter	
4.004 25Jul11	Additional information added on HAD chain	
4.005 16Aug11	Updated chapters: 5/12.2/13/15/17/19/21.3/21.4/21.5/22.1/22.2/ 23.1.2.2/23.1.2.3/23.2.2.2/27 Added chapters: 2.1	
4.101 23Jan12	Updated screenshots, TrustAlert brand replaced with Elephant Security, updated chapters 17, 21, 23, 25, 27	
4.102 17Feb12	Updated chapters 25.2 to 25.6	
4.2 – 19Jun12	Update to KeyTalk Firmware version 4.2 Replaced the product name KeyTalk with KeyTalk. This change in name has not yet been realized in the software.	
4.201 – Aug 2012	Language edited; updated screenshots added; rewrote chapter 22.	
4.202 - 12July13	Updated brand to KeyTalk	



# Table of contents

1.	Intro	duction	7
	1.1.	Getting started	9
	1.2.	Installation 1.2.1. Using the software 1.2.2. Support	
	1.3.	System configurations 1.3.1. Optional configurations	10 10
2.	Front	Panel Components	11
3.	Back	Panel Components	12
4.	Тор Р	Panel Components	13
5.	Quic	c Start Guide	14
	5.1.	Step 1: Powering the appliance	14
	5.2.	Step 2: Connecting the appliance to the internal network	14
	5.3.	Step 3: Connecting to the appliance administrator interface	15
	5.4.	Step 4: Authenticating to the administrator interface	16
	5.5.	Step 5: Set network configuration	17
	5.6.	Step 6: Edit network interface settings	17
	5.7.	Step 7: Change administrator password	17
	5.8.	Step 8: DNS & NTP/Date Time customization	18
	5.9.	Step 9: Save the current configuration	20
	5.10.	Step 10: Connecting the appliance to the external network	21
	5.11.	Step 11: Testing the KeyTalk solution	21
6.	IPv4	and IPv6	24
7.	Setti	ng up the appliance	25
	7.1.	Powering the appliance	25



	7.2. Connecting the appliance to the internal network	25
8.	KeyTalk Admin GUI	26
	8.1. Replacing Admin GUI SSL-certificate	26
	8.2. Saving changes & reboot	27
9.	SSH 29	
10.	Changing KeyTalk passwords	30
11.	Backup and Restore	31
12.	Factory Reset	32
13.	Firmware upgrade	33
14.	Date/time & NTP settings	35
15.	Log files	37
	15.1. Daemon logging settings	38
16.	Network settings	39
	16.1. Configure interfaces	39
	16.2. Configure DNS	41
	16.3. Configure High Availability Virtual Interface	41
	16.4. Configure KeyTalk client listening port	42
17.	Configuring daemons	43
	17.1. Certificate Authority daemon (CAD) settings	43
	17.2. High Availability daemon settings 17.2.1. In depth HA chain	44 45
	17.3. Stop/start daemons & status	46
18.	Services	47
	18.1. Creating/modifying a service	47
	18.2. Hardware Signature	51
19.	Authentication modules	53



	19.1.	Internal	Sqlite database module	53
		19.1.1.	Adding a Sqlite Module to a ser	vice54
		19.1.2.	Changing Sqlite Module setting	s for a service54
	19.2.	LDAP Mo	dule (Includes AD)	59
		19.2.1.	Adding an LDAP Module	
		19.2.2.	Changing an LDAP Module conf	iguration 60
	19.3.	RADIUS		67
		19.3.1.	-	
		19.3.2.	Changing a RADIUS Module con	nfiguration 67
	19.4.	Execute	Modules	70
	19.5.		dules (connecting other authent	
		19.5.1.	- ,	
		19.5.2.		vice configuration 71 
		19.5.3.	Remote exit basics	
	19.6.	Synchror	nize User Lockout List	73
20.	User	messag	es Logged-in users	74
	20.1.	User mes	ssages	74
	20.2.	Logged-i	n Users	75
21.	Licen	se		Error! Bookmark not defined.
22.	Certi	ficates a	and keys configurations	77
	22.1.	Certificat	e Authority	Error! Bookmark not defined.
	22.2.	Requiren	nents	Error! Bookmark not defined.
	22.3.	Signing k	Key	79
	22.4.	25.4 Ser	ver-server Communication Key	80
	22.5.	Client Se	rver Communication Key	81
	22.6.	WebUI C	ertificate & Key	82
	22.7.	KeyTalk	License file	Error! Bookmark not defined.
23.	Error	s and e	ror-reporting	84
24.	LCD i	nformat	tion display	89
25.	Relea	ise note	S	90



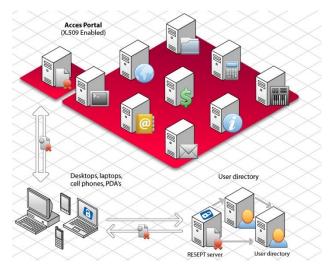
#### 26. Contact information

90

Thanks for choosing KeyTalk (formerly known as RESEPT). This device has been designed to make safe communication the next generation security a reality. On top of that KeyTalk has many additional benefits.

With our patented KeyTalk technology, you can easily provide your entire user community, whether internal or external, with on demand short life X.509v3 certificates.

All built upon your existing infrastructure, so there is no need to change backup procedures, or to teach your community of users new authentication methods.



The KeyTalk appliance simply makes it happen.

KeyTalk provides you with advanced features, which make your life as a user easier and more secure when making use of your company's or partner's online environment.

#### Common usages:

- Single Sign-On to web-based environments
- Digital signing of internal documents
- Highly secure connections to web-based environments
- Protection of your authentication credentials against Man-in-the-Middle attacks
- Optionally binding the computer device(s) to the user or company

X.509v3 user certificates have been the standard since 1988, and are commonly accepted by all Operating Systems. As a result not only do these user certificates enable you the highest level of **safe encrypted communication**, as well as many **more features** with the same ease of management, such as:

- Single Sign-On
- Federated Identity
- 802.1x EAP/TLS



Certificates issued by the KeyTalk appliance work natively with all major and minor network and client brands, such as, but not limited to:

- CISCO
- Juniper
- F5
- Fortinet
- Checkpoint
- SAP
- Microsoft
- Oracle
- Novell

KeyTalk is a product which seamlessly fits into your existing network infrastructure. In a highly secure manner, it automatically creates, distributes, and (de)installs, short living X.509v3 user certificates on the user's device, for the purpose of user credentialing and secure access control.

X.509 is the industry standard since the 80's and is supported by all major network components and enterprise application solutions, and is now made available for short living certificates, making it the perfect unified access control solution. Managing X.509v3 certificates has thus far been one of the greatest cost factors in high secure environments. Cost is now minimized as a direct result of short living certificates, making administrative efforts on Certificate Revocation Lists obsolete.

By re-using your existing authentication environment, optionally leveraging it with trusted corporate hardware recognition, reducing the lifecycle of the certificate, and ultimately automating the certificate requests, creation, distribution and (de)installation, certificate management has become easy as pie with our KeyTalk product.

#### In Short:

KeyTalk protects your data in motion by providing secure access for machine-to-machine communication and data transmissions between devices, corporate networks and cloud applications. It prevents common attacks such as man-in-the-middle. KeyTalk generates, distributes and installs short living client certificates on the client device in a fully automated manner, leveraging your existing authentication methodology. Optionally it uses the device hardware characteristics to strengthen the authentication process.



This document describes how to use the KeyTalk Appliance.

This document is part of the documentation that comes standard with KeyTalk products:

- User manual
- Installation manual
- Prerequisites and Technical requirements
- Quick Reference Guide
- Release notes

#### **1.1. Getting started**

In the following subsections the KeyTalk product is described.

### 1.2. Installation

All our products are delivered with an Installation manual. This manual provides instructions for installing and de-installing the KeyTalk software and gives an overview of the system requirements necessary to run the software. More detailed technical requirements can be found in the Prerequisites and Technical requirement documents.

#### 1.2.1. Using the software

How to use KeyTalk products and an explanation of terminology and icons used in the software are described in detail in the User manual. Next to describing the hardware, the functionalities of the software are also described in full detail. In case of product upgrades an overview of the new functionalities is incorporated in the User manual as well as listed in the product's Release Notes.

For new users of our products, a full training is available for both functional and technical aspects of the solution. Please consult your KeyTalk supplier or KeyTalk partner for more information.

#### 1.2.2. Support

In case you encounter issues when using our products, please contact your KeyTalk supplier. Contact details have been made available to you directly by our partner.



KeyTalk also has a service desk reachable 24/7, but they only provide 3<sup>rd</sup> line support. They can be contacted by e-mail or telephone.

#### Contact details KeyTalk Service desk 3rd line only

E-mail: <a href="mailto:support@keytalk.com">support@keytalk.com</a>

Tel.: +31 64 672 67 94

### 1.3. System configurations

You can have one or more KeyTalk devices configured in **high availability** mode.

#### 1.3.1. Optional configurations

KeyTalk can be used in combination with KeyTalk's DevID appliance.

Within an organization DevID allows the binding up to 10 different hardware signatures of a user's devices to a single unique user. All is done according to the offered authentication service. DevID can be set to automatically learn up to the maximum number of hardware signatures that is allowed per user (setting).

Moreover, DevID is multi-tenant, allowing multiple user groups to be defined per specific KeyTalk authentication services. Each user-group can be separately managed by one or more service operators, allowing one to deploy and manage DevID in a very flexible manner. This way, your Admin does not have to do all the work by themselves.



### Front Panel Components

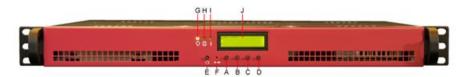


Figure 1. Front	nanol KovTalk	(color of front	bezel may vary)
riguic 1. rione	panel keylak		bezer may vary)

Component	Description
Display navigation button	Controls the navigational controls for the LCD information
А	menu (see section 24 'LCD information display').
Display navigation button	Controls the navigational controls for the LCD information
В	menu (see section 24 'LCD information display').
Display navigation button	Controls the navigational controls for the LCD information
С	menu (see section 24 'LCD information display').
Display navigation button	Controls the navigational controls for the LCD information
D	menu (see section 24 'LCD information display').
Power button	Press to start the device when switched off.
	Press and hold for several seconds to switch off the
	appliance.
RESET button	Press (using a paperclip) and hold for several seconds to
	stop the device. The RESET button only needs to be used
	when normal switch off using the Power button is not
	working.
Power indicator	Lights up when the power is switched on.
Disk indicator	Data is stored on the Solid State Disk. When this indicator
	flashes the Solid State Disk is active.
Information indicator	Lights up when important messages require your
	attention.
LCD Display	Displays the state the device is in and displays menu
	items for local administration.
	Display navigation button A Display navigation button B Display navigation button C Display navigation button D Power button RESET button RESET button Power indicator Disk indicator

Do not replace any components as this will void your KeyTalk warranty.

**Note:** replacing hardware components will result in malfunctioning of the system.



2.

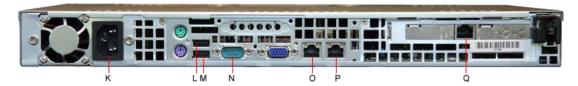


Figure 2: Back panel KeyTalk

3.

	Component	Description
К	Power port	Connector port for the power cable.
L	USB port 1	It is possible to perform functional upgrades via a
		USB key using this USB port.
М	USB port 2	It is possible to perform functional upgrades via a
		USB key using this USB port.
Ν	RS232 port	Manufacturer trouble shooting connector.
0	Network Interface Connector	For connection to other KeyTalk appliances in high
	(NIC)	availability mode, including DEVID. The default IP
		for this connector is 172.16.1.1.
Ρ	Network Interface Connector	For connection to the local management device. The
	(NIC)	default IP for this connector is 10.1.1.1.
Q	Network Interface Connector	For connection to the external network. The default
	(NIC)	IP for this connector is 192.168.1.1.

Do not replace any components as this will void your KeyTalk warranty. *Note:* replacing hardware components will result in malfunctioning of the system.



12

# **Top Panel Components**

On the top panel of the appliance, between the front bezel and the appliance top cover, you will find a blue label.

### 3572321

4.

#### Figure 3: Blue label with appliance's tamper evident serial number

This security label displays the unique appliance tamper evident serial number and should not be removed. It is used for identification purposes in case support is requested.

Removing or otherwise manipulating this label will cause the label to permanently change. KeyTalk advises you to check this label on a regular basis to make sure it is undamaged. Should the label be damaged, please contact your KeyTalk supplier who can provide you with a new label.

In case the label is damaged without your knowledge, be warned that your KeyTalk may have been opened and tampered with. Please report such incident to your KeyTalk administrator and/or security officer.

When the device needs to be sent to the manufacturer for repair, open the device by breaking the label and remove the hard disk. This hard disk contains your company data and should <u>not</u> be sent to the manufacturer. When the device has been repaired, you will receive it back with a new hard disk and label. This hard disk will be in the initial state. Your settings and company data can be restored from a backup. Please refer to the <u>`Backup and Restore'</u> section for more information on how to do this.



#### **Assumptions:**

5.

- The KeyTalk appliance is by default delivered in DEMO configuration and should work immediately after applying the configurations described below.
- For this quick start configuration the default KeyTalk Client should be used together with the DEMO RCCD file. (RCCD: the Remote Configuration Client Data)
- For security reasons the DEMO key and certificate material must always be replaced with production material before taking the solution into a production environment.
- When using production key and certificate material, a corresponding production KeyTalk client RCCD file must be used, otherwise communication will fail. An RCCD file can be generated by your organization itself. This functionality is described in Chapter 5 of the Client Administrator Manual.
- DNS, NTP, HTTP, HTTPS, SysLog, port 3000, and optionally icmp ping 0,8 are assumed to be available for connection purposes.

#### 5.1. Step 1: Powering the appliance

- a) Remove the appliance from its box.
- b) Plug the black power cord into the appliance back power-port 'K'.
- c) Plug the power cable into a power socket-connector.
- d) Press the power-on button (button 'E').

#### 5.2. Step 2: Connecting the appliance to the internal network

The KeyTalk appliance has 3 active Network Interface Connectors (NIC) 'O', 'P' and 'Q' in Figure 2: Back panel KeyTalk.

The NIC 'P' is 10.1.1.1 and is assigned to the KeyTalk management interface. This NIC should only be accessible to the system administrator.

e) Connect the administrator PC/Laptop by UTP cable.



f) Configure the administrator PC/Laptop to the 10.1.1.x network so that you may be able to connect to 10.1.1.1.
 Pick for example the 10.1.1.50 address (address must be 10.1.1.x with x>4) for the administrator PC and use network mask 255.255.255.0.

**NOTE:** By default pre-configuration is based on IPV4, however IPV6 is fully supported. The focus for manuals and training is, however, on IPV4 and will not go into detail for IPV6 configuration.

Sample screenshots on a Windows 7 (64) PC on how to configure your IP:

Local Area Connection Properties	Internet Protocol Version 4 (TCP/IPv4) Properties
Networking Sharing	General
Connect using:	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Configure This connection uses the following items:	O gbtain an IP address automatically           IV use the following IP address:           IP address:           IP address:           Subnet mask:           255 . 255 . 0           Default gateway:
	Olgtain DNS server address automatically     Olgtain DNS server:     Preferred DNS server:     Alternate DNS server:     Alternate DNS server:
wide area network protocol that provides communication across diverse interconnected networks.	Vajdate settings upon exit Advanced
OK Cancel	OK Cancel

Figure 4: IP configuration on a Windows 7 (64bit) PC

# 5.3. Step 3: Connecting to the appliance administrator interface

The KeyTalk appliance Graphical Admin Interface can be accessed by browser over the following URL: <u>https://10.1.1.1:3000</u>.

#### Note: Pay attention to the S in HTTPS and port 3000!

Because the appliance is configured using a self-signed SSL certificate by default, you will likely get a warning that the security certificate was not issued by a trusted certificate authority.

In this case, ignore the warning and continue to the website. This is a workaround!!; a trusted certificate should be obtained from a known certificate authority such as VeriSign, GoDaddy and Cybertrust, or from the KeyTalk Certificate Authority, before going into production. When the certificate is installed, no warning should occur.





Figure 5: Sample warning

You will then go to the login page for KeyTalk.

#### 5.4. Step 4: Authenticating to the administrator interface

The default authentication credentials to access the KeyTalk administrator interface role are:

User: reseptadmin Password: change!

The server 10.1	1.1 at RESEPT ADMIN requires a username and password.
	reseptadmin       Image: september my credentials
	OK Cancel

Figure 6: Login to KeyTalk administration page after ignoring the certificate warning

This user has full access to all the options on the KeyTalk device.

The homepage of KeyTalk will open:

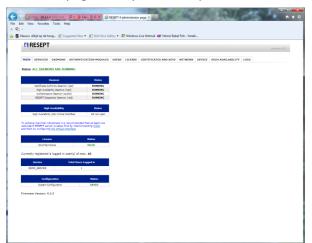


Figure 7: Homepage KeyTalk



#### 5.5. Step 5: Set network configuration

For configuring the network, network administration knowledge is required.

To set the network configuration, select the 'NETWORK' tab in the upper menu, select "Configuration Interface", enable the 'External' checkbox and select "CHANGE".

	Interface Type	IPv4 Address	IPv4 Subnet Mask	IPv4 Configuration	IPv6 Address	IPv6 Prefix Length	IPv6 Configuratio
	Loopback	127.0.0.1	255.0.0.0	Automatic	::1	64	Automatic
	Internal 🚺	172.16.1.1	255.255.0.0	Manual	fd7c::ac10:101	64	Manual
	External 🚺	192.168.1.1	255.255.255.0	Manual	fd7c::c0a8:101	64	Manual
	Management i	10.1.1.1	255.0.0.0	Manual	fd7c::a01:101	64	Manual
Default	t IPv4 Gateway:						
Default							

Figure 8: Setting network configuration

#### 5.6. Step 6: Edit network interface settings

Configure 'IP Address', 'Subnet Mask' and the 'Default Gateway' to match your own network topology and click 'OK' to save these settings.

	_
Interface Type:	External
Ipv4 Configuration:	manual
IPv4 Address:	192.168.1.1
IPv4 Subnet Mask:	255.255.255.0
Ipv6 Configuration:	Manual
IPv6 Address:	fd7c::c0a8:101
IPv6 Prefix Length:	64
ок	CANCEL

Edit Network Interface Settings

Figure 9: Network Interface Settings

**Note:** Optionally you can set a gateway for each NIC separately.

#### 5.7. Step 7: Change administrator password

To guarantee the best security possible, it is important to change all user passwords before step 10 'Connecting the appliance to the external network'.

The Graphical Administrator Interface can be used, when required, for maintenance.



The Admin authentication credentials are by default set to: Graphical Administrator Interface (Admin GUI): User: reseptadmin Password: change!

In order to change the Graphical Administrator Interface password, do the following: In the upper menu select the 'DEVICE' tab and select 'Admin Password'.

MAIN	DAEMONS	AUTHENTICATION MODULES	USERS	LICENSE	CERTIFICATES AND KEYS	NETWORK	DEVICE	HIGH AVAILABILITY	LO
ne   Admin Passwor		Save & Reset Configuration   Ba	skup & Posto	ra Casfiau	ation   Firmware Unarado   Sh	ut Down   Ron			
Hall Admin Passwork	d Ton Access	- Save & Reset Configuration   Ba	ckup & Restu	ire connigui	ation   Pinnware opgrade   Si	ut Down   Kep	ort problen	1	
hange Device V	Veb Access	Password							
Account:	reseptadmin								
Current Password:									
current Password:									
New Password:									
	-								
Repeat New Password:									
ок									
hange Device A	dmin Passy	word							
inange betree A									
Account:	reseptadmin								
Current Password:									
New Password:									
Repeat New Password:									
OK									

#### Figure 10: Changing Graphical Administrator Interface password

Enter both current and new password and confirm the new password in the Change Device Web Access Password fields. Press "OK" to activate the new password. **Note:** It is important to remember this password.

The KeyTalk appliance also has a more powerful user, the device admin, for low level administrator maintenance. This user is not enabled by default. If required, contact your KeyTalk supplier or partner.

#### 5.8. Step 8: DNS & NTP/Date Time customization

To set your applicable **DNS**, select the "NETWORK" tab in the upper menu and select "Configure DNS".

It is possible to ping the IP in order to check if the IP maps to a living machine. Note:

The firewall might block the ping (icmp echo request/reply).

Enter the IP addresses of your DNS and select 'OK'.



0						
Config	ure DNS S	ettings				
Name Se	rver#1		PING			
Name Se	rver#2		PING			
Name Se	rver#3		PING			

Figure 11: Setting the applicable DNS

To set the applicable **date/time**, go to the tab "DEVICE" and select "Time".

Enter the current date and time in UTC(!), and select "SET".

MAIN	SERVICES	DAEMONS	AUTHENTICATION MODULE	S USERS	LICENSE	CERTIFICATES AND KEYS	NETWORK	DEVICE	HIGH AVAILABILITY	
Time   A	min Password	SSH Access	Save & Reset Configuration	Backup & Re	store Configu	ration   Firmware Upgrade   Sh	ut Down   Rep	ort problem		
Config	ure Device	Time								
System	Time: 2012-0	7-26 10:17:45								
Offset fr	om UTC: +00:	00								
5	ET									
Use NTP										
NTP Sen	/er#1									
NTP Sen	/er#2									
NTP Sen	/er#3									
NTP Sen	/er#4									
NTP Ser	/er#5									
NTP Sen	1007F6									
NTP Sen	/er#7									
NTP Sen	/er#8									
	ж									

Figure 12: Setting the applicable date/time

**Note:** The Netherlands is UTC+1 (during summertime UTC+2); CST = UTC-6 (during summertime UTC-5); EST = UCT-5 (during summertime UTC-4).

Preferably set your applicable **NTP server(s)**. When using NTP server(s) also check the 'Use NTP' box. Confirm by selecting "OK".



Configu	ire Device	Time				
System T	me: 2012-07	7-26 10:17:45				
Offset fro	m UTC: +00:	DO				
s	T					
Use NTP		)				
NTP Serve	er#1					
NTP Serve	er#2					
NTP Serve	er#3					
NTP Serve	er#4					
NTP Serve	er#5					
NTP Serve	er#6					
NTP Serve	er#7					
	er#8					

Figure 13: Setting your applicable NTP server(s)

#### **Possible problems**

Please make sure the firewall rules allow connection of NTP services (UDP123). Also keep in mind that NTP will only slowly correct the time settings. This is standard NTP behavior and to avoid a delay, manually set the time before enabling NTP. Manually setting the time cannot be done after enabling NTP.

Also see section 14 '<u>Date/time & NTP settings</u>'. There are two menu items to configure the time, but both function identically. One menu item is located in the 'Network configuration', the other in 'Device configuration'. Both direct you to the same function.

#### 5.9. Step 9: Save the current configuration

In the main menu select the 'DEVICE' tab and select 'Save & Reset Configuration". Select "SAVE" to save the System Configuration.



Figure 14: Saving current system configuration



In case a system reboot is necessary the standard configuration will be used unless the changes have been saved. See section 8 '<u>KeyTalk Admin GUI'</u> for details about making changes to the KeyTalk Admin GUI and saving the changes.

### 5.10. Step 10: Connecting the appliance to the external network

The KeyTalk appliance has 3 active Network Interface Connectors (NIC). These are 'O', 'P' and 'Q' (see section 3 'Back Panel Components').

NIC 'Q' is by default assigned to 192.168.1.1 and to be connected to the external network. This NIC should be used for regular KeyTalk client-server communication.

### 5.11. Step 11: Testing the KeyTalk solution

Now that the installation is complete, the KeyTalk solution can be tested using the provided demo KeyTalk Client in combination with the DEMO RCCD file.

Update the KeyTalk client configuration: start the RESEPT Configuration Manager from the Windows START menu:

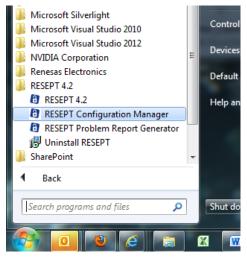


Figure 15: KeyTalk Configuration Manager



() F	RESEPT Configur	ation Manager	
	General		
	Installed Setting	S	
	Provider	User Settings	Master Settings
	Load		
			OK Cancel

Figure 16: RESEPT Configuration Manager

Load the RCCD file to test the KeyTalk appliance by clicking on "Load..."

Load Settings	<b>X</b>
Load Settings	
From URL:	
From File:	
	Load Cancel

Figure 17: Selecting the setting to load a RCCD file

Browse to the location where the RCCD is saved, either via your browser or from your local system.

Click on "Load" to upload the selected RCCD file. After successful upload the following message will appear on screen:

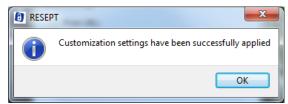


Figure 18: RCCD file was successfully uploaded and applied

If the screen above does not appear, the RCCD file you tried to upload may be corrupt. Please recreate the RCCD file and upload again.

After clicking "OK", the screen below will open:



Select the "Provider Settings" tab and enter the appropriate KeyTalk Appliance server, which can be specified by IP address or DNS name. When done, select "OK".

RESEPT Configuration Manager
General Provider Settings Service Settings
Provider: ElephantSecurity
Server: keymaster.com
Log Level: DEBUG
OK Cancel

Figure 19: Sample provider settings

For testing purposes the KeyTalk internal user database is already configured with a 'DemoUser'. Additional users can be easily added using the Admin GUI, see section 19 'Authentication modules' for more information.



The KeyTalk appliance fully supports IPv4 and IPv6.

Out-of-the-box demo configurations are based on IPv4.

Admins who wish to make use of IPv6 will need to configure the appropriate IPv6 settings.



#### 7.1. Powering the appliance

7.

- 1. Remove the appliance from its box.
- 2. Plug the black power cord into the appliance back power-port ('K').
- 3. Plug the power cable into a power socket-connector.
- 4. Press the power-on button ('E').

### 7.2. Connecting the appliance to the internal network

The KeyTalk appliance has 3 active Network Interface Connectors (NIC) ('O', 'P' and 'Q').

The address of 'P' is by default 10.1.1.1 and is assigned to the KeyTalk administrator interface.

Follow these steps to connect the appliance to the internal network:

- Connect the administrator PC/Laptop by UTP cable.
- Configure the administrator PC/Laptop to the 10.1.1.0 network so that you are able to connect to 10.1.1.1.
- Sample screenshots on a Windows 7 (64) PC on how to configure your IP from Local Area Connection Properties:

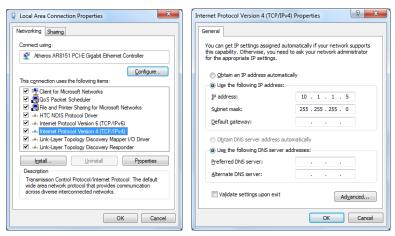


Figure 20: Configure your IP



The KeyTalk appliance Graphic Admin Interface can be accessed with a browser using the following URL: <u>https://10.1.1.1:3000</u>

#### Note: Pay attention to the S in HTTPS and port 3000!

User: reseptadmin

8.

The default password was `change!', but this was changed under section 10 <u>`Changing</u> <u>KeyTalk passwords</u>'. Please remember to use your new password.

Because the appliance is configured to use a self-signed SSL certificate by default, you will likely to get a warning that the security certificate was not issued by a trusted certificate authority. In this case, ignore the warning and continue to the website.

Sample warning:	There is a problem with this website's security certificate.
	The security certificate presented by this website was not issued by a trusted certificate authority. The security certificate presented by this website was issued for a different website's address.
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
	We recommend that you close this webpage and do not continue to this website.
	Ø Click here to close this webpage.
	Continue to this website (not recommended).

To avoid this warning you must install a certificate from a trusted party such as VeriSign, GoDaddy, GlobalSign, Cybertrust, or from your own KeyTalk Certificate Authority. See following section for details.

#### 8.1. Replacing Admin GUI SSL-certificate

By default a self-signed SSL certificate is used to access the appliance over <u>https://10.1.1.1:3000</u>

You should replace this SSL certificate with your own. A certificate can be obtained from a well-known party such as VeriSign, GoDaddy, Globalsign and Cybertrust.

In the main menu, select "CERTIFICATES AND KEYS" and select "WebUI". Upload your own SSL certificate by clicking on "Browse...", selecting the SSL certificate and clicking on "UPLOAD".



MAIN SERVIC	ES DAEMONS	AUTHENTICATION MODULES	USERS	LICENSE CERTIFICATES AND KEYS NETW	DRK DEVIC	E HIGH AVAILABILITY	LOG
verview   Root CA	Primary CA	Signing CA   Communication CA   Se	rver-Serve	er   Client-Serfer   WebUI   Server-DevId   DevId W	bUI   Backup	& Restore   Generate	
VebUI certificate	and key are us	sed to secure access to the RESEP	PT server	UI via browser.			
Certificate Info							
Subject:	C=NL ST=Utre	cht L=Soesterberg O=Resept Demo OU=	Demo Only	CN=reseptadmin.reseptdemo.com emailAddress=demo@	eseptdemo.com		
Issuer:	C=NL ST=Utre	cht L=Soesterberg O=Resept Demo OU=	Demo Only	CN=Resept Demo CCA emailAddress=demo@reseptdemo	com		
Valid From:	22-03-2011 13	3:34 ( 22-03-2011 13:34 GMT )					
Valid To:	17-05-2027 13	8:34 ( 17-05-2027 13:34 GMT )					
Signature Algorithm	sha1WithRSAE	ncryption					
Public Key:	RSA (2048 bits	)					
SHA1 Fingerprint:	24339f015e2cf	046a7ba95ef0c1df5fe7af9045a					
Type: RSA (2048   Jpload Certific Click "Upload" to UPLOAD	ate and Key	ntaining certificate and key. The l	key shoul	d not be protected with password.			
	to download c	ertificate and key as a single PEM	file.				
DOWNLOAD							
he device manage	ment interface r	may automatically restart after the ce	ertificate/k	ey file is uploaded.			
	Danla	sing the CCL con					

Figure 21: Replacing the SSL-certificate

Make sure that the SSL certificate you wish to make use of, also contains the private key, and is in a PEM file format.

Select the file by pressing BROWSE and press UPLOAD to replace the existing SSL certificate.

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new SSL certificate.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.

### 8.2. Saving changes & reboot

Changes made in the Admin GUI will be effective, as long as the KeyTalk appliance does not lose its electric power. In order to make changes permanent, the changes must be saved by the administrator.

**SAVING:** In the main menu select the "DEVICE" tab and select "Save & Reset Configuration". Select "SAVE" to save the System Configuration.



MAIN	SERVICES	DAEMONS	AUTHENTICATION MODULES	USERS	LICENSE	CERTIFICATES AND KEYS	NETWORK	DEVICE	FIGH AVAILABILITY	LOGS
Time   A	lmin Password	SSH Access	Save & Reset Configuration	ckup & Res	store Configu	ration   Firmware Upgrade   Sh	ut Down   Rep	port Problem		
Save S	ystem Con	figuration								
			ystem configuration to non-vola equals to the saved configuration							
	VE	)								
Reset	Configurati	on To Fact	ory Defaults							

#### Reset Configuration To Factory Delauits

Click "Reset" to reset the current system configuration the factory defaults.

 RESET

 The device will automatically reboot when the configuration is reset.

Figure 22: Saving System configuration

#### REBOOT: In the main menu select the "DEVICE" tab and select "Shut Down". Select

"REBOOT" to reboot the system.

 MAIN
 SERVICES
 DAEMONS
 AUTHENTICATION MODULES
 USERS
 LICENSE
 CERTIFICATES AND KEYS
 NETWORK
 DEVICE
 Did Availability
 Logs

 Time
 Admin Password
 SSH Access
 Save & Reset Configuration
 Backup & Restore Configuration
 Firmware Upgrad
 Shut Down
 Report Problem

REBOOT SHUT DOWN

Figure 23: Rebooting the system



SSH is by default disabled on the KeyTalk appliance. Should there be a need to activate it, please contact your KeyTalk supplier for an updated KeyTalk license with activated SSH.



# 10. Changing KeyTalk passwords

The Graphical Administrator Interface can be used, when required, for administrator maintenance.

The Admin authentication credentials are by default set to: Graphical Administrator Interface (Admin GUI):

User: reseptadmin

Password: change!

In order to change the Graphical Administrator Interface password, do the following: In the upper menu select the 'DEVICE' tab and select 'Admin Password'.

MAIN SERVI	CES DAEMONS	AUTHENTICATION MODULES	USERS LICENSE	CERTIFICATES AND KEYS	NETWORK	DEVICE	HIGH AVAILABILITY	LOGS
ime   Admin Pass	sword   SH Access	Save & Reset Configuration   Ba	ckup & Restore Config	uration   Firmware Upgrade   Sh	nut Down   Rep	ort Problem		
hange Devic	ce Web Access	Password						
Account:	reseptadmin							
Current Password:								
New Password:								
epeat New Passw	rord:							
ок Change Devic	ce Admin Pass	word						
Account:	reseptadmin							
Current Password:								
New Password:								
Repeat New Passw	rord:							
ОК								

#### Figure 24: Changing Graphical Administrator Interface password

Enter both current and new password, and confirm the new password, in the Change Device Web Access Password fields. Press "OK" to activate the new password. **Note:** It is important to remember this password.

The KeyTalk appliance also has a more powerful user, the device admin, for low level administrator maintenance. This user is not enabled by default. If required, contact your KeyTalk supplier or partner.



### 11. Backup and Restore

To make a full backup of your current system configuration to your computer, select "DEVICE" from the main menu, select "Backup & Restore Configuration" and select "BACKUP".



Figure 25: Making a backup of the system configuration

Save the backup file "resept.config\_dat" in a location of your choice.

To restore your backup of your system configuration, select "DEVICE" from the main menu, select "Backup & Restore Configuration" and select "Browse" under 'Restore Configuration'.

Select your "resept.config.dat" backup file, and select "RESTORE". The KeyTalk appliance will reboot afterwards, to effectuate the changes.

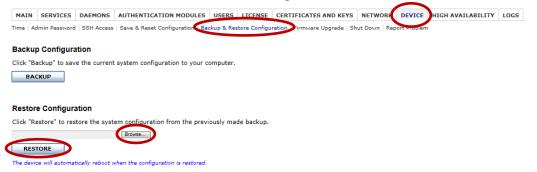


Figure 26: Restoring the system configuration backup file



# 12. Factory Reset

Should you ever want to reset the KeyTalk appliance to its original factory settings, the steps described below must be followed.

Select from the main menu the "DEVICE" tab and select "Save & Reset Configuration". Select "RESET" to restore default factory configuration settings.



Figure 27: Resetting the Factory Defaults

**Note:** When resetting the default factory configuration settings, this will also affect your set IP addresses!! In case your KeyTalk device is off premise, remote communication with the device will be impossible after a factory reset.



KeyTalk BV releases periodically new firmware for the KeyTalk appliance.

New firmware can fix bugs as well as add new functionality.

Upgrading requires you to go from one version to the next in full sequential order. Skipping a firmware version in between may result in the malfunctioning of the KeyTalk appliance.

**Note:** Before upgrading your firmware, make sure the Daemons are stopped. See section 17 '<u>Configuring daemons</u>' in case you update a live system.

Upgrading the KeyTalk firmware can be done in two different ways:

1. For remote upgrading, you can upload the upgrade-file via the administrator graphical interface (Admin GUI).

Within the KeyTalk Admin GUI, go to "DEVICE", select "Firmware Upgrade", click on 'Browse' to select the upgrade-file and click on "UPLOAD" to start the upgrade process.

MAIN	SERVICES	DAEMONS	AUTHENTICATION MODULES	USERS	LICENSE	CERTIFICATES AND KEYS	NETWORI DE	VICE	IGH AVAILABILITY	LOGS
Time   Ad	dmin Password	SSH Access	Save & Reset Configuration   Ba	ckup & Re	store Configu	uratio Firmware Upgrade Dh	ut Down   Report P	roblem		
Current	Firmware Ve	rsion: 4.2.0								
To insta	l upgrade ple	ase do ONE	of the following:							
• Fither	upload RESE	PT image to t	he server							
			Browse							
UP	LOAD	>								
• Or sta	rt upgrade da	emon and in	sert USB stick with resept.img							
s	TART									
Your con	figuration will	be automatica	lly saved during upgrade.							
			when the upgrade is complete.							

#### Figure 28: Firmware upgrade - remote

2. If you have physical access to the appliance, you can use a USB-stick for the upgrade.

Within the KeyTalk Admin GUI, go to "DEVICE", select "Firmware Upgrade", insert the USB stick with the upgrade-files on it into one of the USB ports 'L' or 'M', the LCD menu will be activated. Click on "START" to upgrade. The system will HALT after an upgrade, requiring an additional reboot.



MAIN	SERVICES	DAEMONS	AUTHENTICATION MODULES	USERS	LICENSE	CERTIFICATES AND KEYS	NETWOR	DEVICE	IGH AVAILABILITY	LOGS	
Time   Ad	lmin Password	SSH Access	Save & Reset Configuration   Bac	kup & Res	store Configu	uratio 🔰 Firmware Upgrade Dh	ut Down   Rep	ort Problem			
Current	Firmware Vei	rsion: 4.2.0									
ro instal	l upgrade ple	ase do ONE (	of the following:								
Either	upload RESE	PT image to t	he server								
	LOAD										
	t upgrade da TART	emon and in:	sert USB stick with resept.img								
Your con The devi	figuration will i te will automai	be automatica tically reboot v	lly saved during upgrade. when the upgrade is complete.								

Figure 29: Firmware upgrade – on premise

As a result the upgrade will start. The progress of the upgrade will be shown in the Admin GUI.

On successful upgrade, the appliance will automatically REBOOT to apply the new firmware.



# 14. Date/time & NTP settings

To set the applicable **date/time**, go to the tab "DEVICE" and select "Time". Enter the current date and time in UTC (!), and select "SET". The KeyTalk appliance will do all required time zone calculations.

MAIN	SERVICES	DAEMONS	AUTHENTICATION	MODULES	USERS	LICENSE	CERTIFICATES AND	KEYS NETWOOK	DEVICE	HIGH AVAILABILITY
Time   Al	min Password	SSH Access	Save & Reset Config	guration   Bac	kup & Res	store Configu	ration   Firmware Upgra	ade   Shut Down   Re	eport Problem	
Configu	ire Device	Time								
System Ti	ime: 2012-0	7-26 10:17:45								
Offset fro	m UTC: +00:	00								
SE	т									
Use NTP										
NTP Serve	er#1									
NTP Serve	ar#2									
NTP Serve	er#3									
NTP Serve	er#4									
NTP Serve										
NTP Serve	er#6									
NTP Serve	er#7									
NTP Serve	er#8									
NTP Serve										

Figure 30: Setting the applicable date/time

**Note:** The Netherlands is UTC+1 (during summertime UTC+2); CST = UTC-6 (during summertime UTC-5); EST = UCT-5 (during summertime UTC-4).

It is highly recommended to set your applicable **NTP server(s)**. When using NTP server(s) also check the 'Use NTP' box. Confirm by selecting "OK".



Time   Id	min Password	DOH Access	Save of Rest	ecconfiguration	backup of Re	store conligu	ration   Firmware	opgrade   Si	de bown   Ke	port Problem	
Configu	ire Device	Time									
System Ti	me: 2012-07	7-26 10:17:45									
Offset from	m UTC: +00:0	00									
SE	1										
Use NTP											
NTP Serve	er#1										
NTP Serve	ar#2										
NTP Serve	er#3										
NTP Serve	er#4										
NTP Serve	v#5										
NTP Serve	er#6										
NTP Serve	er#7										
NTP Serve											
NTP Serve	si ** 0										

Figure 31: Set your applicable NTP server(s)

See section 5.8 '<u>Step 8: DNS & NTP/Date Time customization</u>' for details on setting the time for DNS and NTP. There are two menu items to configure the time, but both function identically. One menu item is located in the 'Network configuration', the other in 'Device configuration'. Both direct you to the same function.



The log files of the four main Daemons and the Web UI can be accessed from the tab "LOGS" in the upper menu:

- AUTHD Logs Authentication daemon logs
- CAD Logs Certificate Authority daemon logs
- HAD Logs High Availability daemon logs
- RDD Logs RESEPT Distribution daemon logs
- WebUI Logs Web interface logs

For example, from the main menu, select the "LOGS" tab and select "AUTHD Logs".

MAIN	SERVICES	DAEMONS	AUTHENTICATION MODULES	USERS	LICENSE	CERTIFICATES AND KEYS	NETWORK	DEVICE	HIGH AVAILABILITY LOGS
AUTHD L	.ogs   AD Log	s   HAD Logs	RDD Logs   WebUI Logs						
Auth D	aemon Log	naina Setti	nas						
			192						
Log Loca		•							
Logging									
Log Seve	erity: debug	•							
	ж								
					A	n Daemon log (last 500 entries)			
					Auto	r Daemon log (last 500 entries)			
			_						
REF	RESH	CLEAN							

Figure 32: Authentication daemon logs



# 15.1. Daemon logging settings

Each Daemon and the Web UI have their own log file that can be configured individually.

#### Auth Daemon Logging Settings

Log Location:	local 💌
Logging Host:	
Log Severity:	debug 💌
ОК	

#### Figure 33: Daemon logging settings, e.g. for the authentication daemon log

Log Location allows the Admin to choose between local logging (default) and remote logging.

When local logging is chosen, the appropriate Daemon's log file will be stored on the local KeyTalk appliance until it reaches a 250k size. After that the local log file rotates to a fresh log file.

Choosing remote logging requires setting a host. Remote logging will allow for a continuous log file on your syslog-server.

Log Severity allows from minimal logging using the "emerg" (= emergency), to the standard log level of "err" (=error), up to the most comprehensive log file under the "\*" setting.



# 16.1. Configure interfaces

To configure the network, network administration knowledge is required.

The KeyTalk appliance makes use of four interfaces. These can be configured by selecting from the main menu "NETWORK", followed by selecting "Configure Interfaces".

	Interface Type	IPv4 Address	IPv4 Subnet Mask	IPv4 Configuration	IPv6 Address	IPv6 Prefix Length	IPv6 Configuration
]	Loopback	127.0.0.1	255.0.0.0	Automatic	::1	64	Automatic
]	Internal 🚺	172.16.1.1	255.255.0.0	Manual	fd7c::ac10:101	64	Manual
]	External 🚺	192.168.1.1	255.255.255.0	Manual	fd7c::c0a8:101	64	Manual
]	Management 🚺	10.1.1.1	255.0.0.0	Manual	fd7c::a01:101	64	Manual
	v4 Gateway:						
	v6 Gateway:						

Figure 34: Configuring interfaces

#### **Interface Types**

Loopback:	cannot be configured from the Admin GUI
Internal:	corresponds to NIC "O", see Section 3 'Back Panel Components'
External:	corresponds to NIC "Q", see Section 3 'Back Panel Components'
Management:	corresponds to NIC "P", see Section 3 'Back Panel Components'

To configure a specific interface, select the appropriate box and click on "CHANGE".

Interface Type	IPv4 Address	IPv4 Subnet Ma
Loopback	127.0.0.1	255.0.0.0
Internal 🚺	172.16.1.1	255.255.0.0
External 🚺	192.168.1.1	255.255.255.0
Management 🚺	10.1.1.1	255.0.0.0

Figure 35: Changing the Internal Interface type



#### Edit Network Interface Settings

Interface Type:	Internal	
Ipv4 Configuration:	manual	
IPv4 Address:	172.16.1.1	
IPv4 Subnet Mask:	255.255.0.0	
Ipv6 Configuration:	Manual	
IPv6 Address:	fd7c::ac10:101	
IPv6 Prefix Length:	64	
Changing the interr	al interface settings will cause all running RESE	T daemons bound to the internal interface to resta
ок	CANCEL	

Figure 36: Edit Network interface settings

Configure the items you wish to change and select "OK" to save these changes.

To change the KeyTalk appliance default gateway, select from the main menu "NETWORK", select "Configure Interfaces" and select "CHANGE".

Interface Type	IPv4 Address	IPv4 Subnet Mask	IPv4 Configuration	IPv6 Address	IPv6 Prefix Length	IPv6 Configuratio
Loopback	127.0.0.1	255.0.0.0	Automatic	::1	64	Automatic
Internal 🚺	172.16.1.1	255.255.0.0	Manual	fd7c::ac10:101	64	Manual
External 🚺	192.168.1.1	255.255.255.0	Manual	fd7c::c0a8:101	64	Manual
Management 🚺	10.1.1.1	255.0.0.0	Manual	fd7c::a01:101	64	Manual
v4 Gateway:						

Figure 37: Changing default Gateway

Change Default Gateway

On the screen that opens, configure the default gateway IP and select "OK".

Default IPv4 Gatev	way:			
		CANCEL	_	
OK		CANCEL		
OK		CANCEL		

Setting the default gateway has effect only when all non-loopback interfaces that use manual (i.e. non-DHCP) configuration

#### Figure 38: Changing the default gateway

**Note:** Optionally you can set a gateway for each NIC separately.



# **16.2.** Configure DNS

To set your applicable DNS, from the upper menu select "NETWORK" and select "Configure DNS".

		$\sim$							
Config	ure DNS S	ettings							
Name Se					PING	Г			
Name Se	erver#1				PING				
Name Se	erver#2				PING				
Name Se	erver#3				PING				
Activatin	g DHCP client	will overwrite	the Name Servers Setting:	s above					

Figure 39: Configuring your DNS

Enter the IP addresses of your DNS and select 'OK'.

**Note:** Do not enter your host name, but your IP addresses.

# 16.3. Configure High Availability Virtual Interface

When running multiple KeyTalk chains (i.e. split daemons on multiple KeyTalk appliances) you may wish to setup a redundancy group. For more info on KeyTalk chains refer to section 17.2.1 <u>In depth HA chain</u>.

One logical KeyTalk server consists of one or more physical KeyTalk appliances (servers) grouped by the same redundancy group ID. From the KeyTalk Client perspective it behaves as one server with one IP address. This IP address is provided by a virtual interface called High Availability (HA) interface.

On one appliance the daemons are configured in chains. If the chain breaks, the master appliance will communicate this to the other appliances within the same redundancy group in order to elect a new master.

High Availability is not a substitute for load balancing. The current limitation of the High Availability for the KeyTalk appliance is that it is bound to one network ip-range.

To configure the High Availability, from the main menu select "NETWORK", then select "Configure HA Interface".



MAIN	SERVICES	DAEMONS	AUTHENTICATION	N MODULES	USERS	LICENSE	CERTIFICATES	ND KEYS	NETWORK	DEVICE	HIGH AVAILA	BILITY	LOGS	
Configure	Interfaces   C	onfigure DN	Configure HA Inter	face Configu	ire RESEPT	Client Liste	n Port   Configure N	гр	$\smile$					
Config	ure High Av	ailability V	/irtual Interface											
a virtual	interface call	ed High Avai	rvers you may wish ilability (HA) interfa nsparently for all Ri	ace. If any se	erver from	cy group. A the group	redundancy group stops working (e.e	consists o , because	f several RE of planned i	ESEPT serve maintenanc	rs accessible for e or fail-stopped	r RESEPT I daemor	r clients n), anoth	via a single IP p her server autom
HA Config	guration: 🗓	disabled												
Virtual In	terface Status:	i down												
Redundar	ncy Group Id: 🛙	4												
Ipv4 Cont	figuration:	Manual												
IPv4 Add	ress:	192.168.1	1.90											
IPv4 Sub	net Mask:	255.255.2	255.0											
	figuration:	Manual												
TDAP COUL		fe80::200	0:5eff:fe00:104%6											
IPv6 Add	ress:													

Figure 40: Configuring the High Availability Virtual Interface

Make the appropriate configuration changes and select "OK".

# 16.4. Configure KeyTalk client listening port

It is very unlikely that you will have to change the port number on which the KeyTalk appliance listens to the KeyTalk Client; as the default 80 port will pass most firewalls. If you would like to change the port, select from the main menu "NETWORK", and select "Configure RESEPT Client Listen Port".

aces   Configure DNS	Configure HA Inter	ce   Configure RES	EPT Client Lister	n Port   Onfigure NTP		
ESEPT Client Lis	ten Port					
External						
192.168.1.1						
fd7c::c0a8:101						
	External 192.168.1.1	192.168.1.1	External 192.168.1.1	External 192.168.1.1	External 192.168.1.1	External 192.168.1.1

Figure 41: Configuring the KeyTalk client listening port

Change the port number and select "OK" to save the change. Additionally you must change the KeyTalk client RCCD file to contain the corresponding port number for the INI file(s).



# 17. Configuring daemons

In Unix and other multitasking computer operating systems, a daemon is a computer program that runs as a background process, rather than being under the direct control of an interactive user (*source: Wikipedia.org*).

The following daemons are important for proper functioning of the KeyTalk appliances:

# • AUTHD – Authentication daemon

Responsible for the user authentication process. It will connect to the applicable authentication database.

• CAD- Certificate Authority daemon

The actual creator of the certificate. It will be invoked after successful authentication.

• HAD- High Availability daemon Responsible for the high availability functionality of the KeyTalk solution.

# • RDD – RESEPT Distribution daemon

User traffic connects to the RDD. This daemon will sanitize the user input, perform some checks and when correct, will take responsibility for the distribution of the workflow to the other daemons.

Next to the above mentioned daemons, there is also an Admin GUID daemon running on the KeyTalk appliance.

Two daemons, CAD and HAD, can be configured in the tab "DAEMONS".

 MAIN
 SERVICES
 DAEMONS
 AUTHENTICATION MODULES
 USERS
 LICENSE
 CERTIFICATES AND KEYS
 NETWORK
 DEVICE
 HIGH AVAILABILITY
 LOGS

 CAD Settings
 HAD Settings
 Status
 Status

#### Figure 42: Configuring daemons

In the next sub-sections it is described how these two daemons can be configured.

# 17.1. Certificate Authority daemon (CAD) settings

To configure the Certificate Authority daemon, select "CAD Settings" in the "DAEMON" tab.



	MAIN	SERVICES	DAEMO		THENT	ICATIO	
<	CAD Sett	ings HAD Settin	ngs   S	tatus			
	Config	ure CAD Sett	tings				
	Save Sig	ning Key Password	. i	<b>V</b>			
	Signing H	Key Password:		•••••			
	C	ж					

Figure 43: Configuring the CAD Settings

The CAD is responsible for the creation of the user certificates and keys.

When a password is present on your CAD Signing Key you may wish to store it for REBOOT purposes. The default password on the KeyTalk DEMO is blank.

Select "OK" to save.

# 17.2. High Availability daemon settings

To configure the High Availability daemon, select "HAD Settings" in the "DAEMON" tab.



Configure HAD Settings

Had Sync Service: 🗓	
Binding Interface Type:	Loopback 💌
Binding Port:	7001
ОК	

Figure 44: Configuring the HAD Settings

The HAD is responsible for discovery and synchronization between the other physical KeyTalk appliances.

Select the Binding Interface Type:

- Loopback
  - (See Section 16.1 '<u>Configure interfaces</u>' for the description of this interface type)
- Internal

(See Section 16.1 '<u>Configure interfaces</u>' for the description of this interface type)

Select "OK" to save the new settings.



**Note:** High Availability daemons from other KeyTalk chains will need to be made known to the KeyTalk in order for HAD to work properly.

#### HADs From Other RESEPT servers

	HadSyncService Host	HadSyncService Port
ADD	]	

#### Figure 45: HADs from other KeyTalk servers need to be made known

Select "ADD" to add a new KeyTalk appliance.

#### Add New HAD Connection

HadSyncService Host:	
HadSyncService Port:	
ОК	CANCEL

#### Figure 46: Add new HAD connection

Enter the HadSyncService Host and Port.

Select "OK" to save the settings.

# 17.2.1. In depth HA chain

The KeyTalk High Availability chain allows for a complete set of KeyTalk daemons, to be made available in case of redundancy requirements.

Each chain is a self-supporting chain running on a single KeyTalk appliance. When one component of the chain fails, the HAD will assume the entire chain to be invalid. On initial power-up all appliances will boot up in 'slave-status'. If there is no master in the group, it will be elected automatically. One KeyTalk appliance will become the master. If the master dies the election will be done again as described earlier.

**Note:** High Availability functionality is not a replacement for load balancing functionality.

An example of a HA implementation could be:



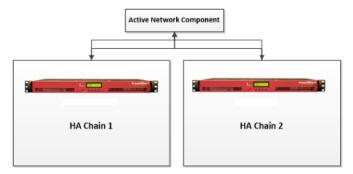


Figure 47: Example HA implementation

Each chain must be configured with the static information. All dynamic information (certificate serials, users etc.) is automatically synchronized, as soon as the chains have been configured to be aware of each other.

To ease configuration, it is a good starting point to always configure one single KeyTalk appliance, and make a backup of its configuration.

**Note:** A configured copy might cause conflicting IP's, so configure with care.

# 17.3. Stop/start daemons & status

AD Settings   H	AD Setting Status			
Daemon	Effective Listen Interface Type	Status	Signing Key Password	Action
authd		running		STOP
cad		running	••••••	STOP
had	HadSyncService: Loopback (IPv4: 127.0.0.1, IPv6: ::1)	running		STOP
rdd		running		STOP

MAIN SERVICE DAEMONS JUTHENTICATION MODULES USERS LICENSE CERTIFICATES AND KEYS NETWORK DEVICE HIGH AVAILABILITY LOGS

The main daemons can be stopped / started from the status panel.

Figure 48: Stop/start daemons & status

When the CAD is started the Signing Key password may need to be entered when the password has been implemented.

To alleviate work for the Admin, it is possible to store the password. This can have security implications, but it has been made available to fit the company's security policy.

How to store the CAD signing key password is described in section 17.1 <u>`Certificate</u> Authority daemon (CAD) settings'.



A service is a group of users that follow the same authentication method and certificate time-to-live. Usually this group of users belongs to the same department/organization.

Services define default values you wish to make available in the client X.509v3 certificates created, distributed and installed by KeyTalk. An example value for the organization attribute is O' = Example.com'.

Additionally attributes in the certificate can be mapped to AD fields.

Multiple services can be configured, allowing you to set up a multitude of services on a single KeyTalk instance.

# 18.1. Creating/modifying a service

To manage services, select from the main menu "SERVICES".

An overview of the existing services is displayed. In this overview, you will find a summary of the services' settings and applicable comments.

The following options are available for Services:

- Add Click on "ADD"
  - Modify Select the existing service and click on "CHANGE"
- Delete
   Select the existing service and click on "REMOVE"

MAN	SERVICES	DEMONS	AUTHENTICA	TION MODULES	USERS	LICENSE	CERTIFICATES	AND KEYS	NETWORK	DEVICE	HIGH AVAILABILITY	LOGS		
	Name	Required Credentials	Key Size	URI		eck IRI	Execute Synchronously		HWSIG Form	ula	Split Domain and Userid	Add	CN Random Chars	Comment
DEMO	D_SERVICE	USERID, HWSI PASSWD	G, 1024	https://www.goog	le.nl			1,2,2,3,4,5	,6,7,8,9,10,11,1	12,13,14,15,1	.6			
AD	DD	CHANGE	REMO	VE										

Figure 49: Adding/modifying/deleting a service

The following pages describe all the fields of the service.



MAIN	SERVICES	DAEMONS	AUTHENTICATION MODULES	USERS	LICENSE	CERTI
	DENTROLD	Differionio		00000	LAULINDL	

#### Edit Service

1	Service Name:	DEMO_SERVICE
2	Required Credentials:	USERID HWSIG PASSWD
3	Key Size (bits):	1024
4	URI:	https://onpremise.elephantsecurity.com
5	File URI Digest:	<b>i</b>
6	Check URI:	
7	Execute Synchronously:	
8	HWSIG Formula:	1,2,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16
9	Split Domain and Userid:	Ē
10	Add 3 Random Characters to CN:	<b>i</b>
11	Country:	NL
12	State:	Utrecht
13	City/Locality:	Utrecht
14	Organization:	Elephant Security Test
15	Organizational Unit:	Test Only
16	Email:	webmaster@keymastertest.com
17	Time To Live (sec):	3600
18	Time For Correction (sec):	-3600
19	Basic Constraints:	CA:FALSE
20	Key Usage:	digitalSignature       Image: nonRepudiation         keyEncipherment       Image: nonRepudiation         keyAgreement       Image: nonRepudiation
21	Extended Key Usage:	ClientAuth Additional OIDs (comma-separated):
	Subject Alternative Name:	
22	nsBaseUrl (contains service name):	DEMO_SERVICE
23	Comment:	
24	OK CANCE	L

Figure 50: Edit a service



1	Service Name	The name assigned to the Service.
		Select what authentication process and credentials are required.
	Required	UserID and HwSig (Hardware signature) are always on and will be
2	Credentials	sent from the client to the server; PASSWD (password), PIN, and
	cicacitatio	(Challenge)RESPONSE are all optional.
		Use the dropdown list to select the preferred RSA key length: 512, 1024, 2048 or 4096 bits.
2	Koy Sizo (hita)	
3	Key Size (bits)	Note that the key size should not exceed the chosen key length of
		the CAD daemon signing certificate. If in doubt about the correct
		key size, consult your KeyTalk supplier or partner.
		This is the URI pushed from the KeyTalk appliance to the KeyTalk
		Client using the specific service. Leave empty when nothing needs
		to be invoked.
		When using a URL it can be used to trigger the KeyTalk client
		when an appropriately supported browser goes to the specific
		base URL. For example: <u>https://webdemo.reseptdemo.com.</u>
		Alternatively when the KeyTalk client has obtained the certificate,
		the client will start the specified URI.
		Instead of a URL the URI can also contain a reference to a local
4	URI	file or program. For example file://yourfilelocation/yourfilename.
		<i>Note:</i> environment variables are respected.
		Starting a program filename can also be done using parameters.
		Note that " " must be used when spaces are included in a path or
		using space separated parameters.
		S - F
		<b>Note:</b> Be careful not to use http:// addresses as these are not
		secure.
5	File URI Digest	Optional field containing the SHA-256 of "file://" URI
		Tick to force a verification of the URI.
		When a URL is used, the IP needs to match both server and client
		side.
6	Check URI	When an executable is started the SHA-256 will be calculated and
		verified. For all the other URI schemes, including empty URI, no
		verification is performed.
		When the URI is an executable, this option allows you to set the
	Execute	
7		client to run synchronously (KeyTalk client will run until
	Synchronously	executable finishes) when selected or a-synchronously when not
		selected.



		The HwSig formula results in a hash calculated over the chosen
		components. This hash is optionally used provided the feature is
		activated in the "Required Credentials" of the Service.
		The formula is comma separated and can contain the HwSig
8	HwSIG Formula	component number references in any order and as often as you
		like. Do note that order and repetition of component numbers
		matter.
		For example: 0,1,2,3,4,5 or 0,0,0,6,7,3,3,8,9,14,11
		For more information on the HwSig, please refer to Section 18.2
		'Hardware Signature'.
		Indicates whether an authentication module should split a fully-
9	Split Domain	qualified userid supplied as domain\userid on two separate
5	and Userid	credentials. Currently only LDAP authentication module supports
		domain credentials.
	Add 3 Random	When selected three random characters are added to the Common
10	Characters to	Name of the generated user certificate. This option is only needed
	CN	for backward compatibility.
11	Country	The default value of the country code (ISO 3166 standard) as it
11	Country	should occur in the user certificate.
12	State	The default value of the state, county or province as it should
12	State	occur in the user certificate.
13	City/Locality	The default value of the city/locality as it should occur in the user
13	City/Locality	certificate.
14	Organization	The default value of the organization as it should occur in the user
14	Organization	certificate.
15	Organizational	The default value of the organizational unit as it should occur in
12	Unit	the user certificate.
10	Ene e il	The default value email address of the organization as it occurs in
16	Email	the user certificate.
47	Time To Live	The default amount of time, expressed in seconds, that a
17	(sec)	certificate is valid from the time it was issued.
	Time For	The default time correction factor, expressed in seconds, to
18	Correction (sec)	correct problems when the Client system time is slightly off.
		CA:FALSE = The generated certificate is a user certificate.
19	Basic	CA:TRUE = The generated certificate is a CA certificate and is
	Constraints	allowed to issue certificates (for advanced use only).
		digitalSignature = Allows for digital signing
		nonrepudiation = <i>Qualifies a digital signature for non-repudiation</i>
20	Key Usage	keyEncipherment = Allows for encryption of keys
		dataEncipherment = $Allows$ for encryption of data
		keyAgreement = Allows for SSL/key handshaking
21	Extended Key	Used for 802.1x EAP/TLS user certificate based authentication.



	Usage	Additional OIDs (comma-separated): Refer to
		http://www.openssl.org/docs/apps/x509v3_config.html#Extended
		<u>Key Usage</u> for more information.
	Subject	The default value of the alternative subject name. For more values
22	Alternative	refer to:
22		http://www.openssl.org/docs/apps/x509v3_config.html#Subject_
	Name	Alternative Name for more information.
	nsBaseURL	Optional Netscape Base URL extension (see MSDN topic:
23	(contains	http://msdn.microsoft.com/en-
	service name)	us/library/aa378149%28v=vs.85%29.aspx for more information.
24	Comment	Free text allowing for comments for Admin support purposes. This
27	Comment	field will not be added to the certificate.

**Note:** Key Usage fields should only be manipulated when you are familiar with their exact functionality and the impact they might have on application/server functionality. For more information refer to RSA-Labs (<u>http://www.rsa.com/rsalabs/</u>) and RFC 5280 (<u>http://tools.ietf.org/html/rfc5280</u>).

**Note:** If not familiar with the exact functionality, it is advised to use the KeyTalk default values for the certificate attributes.

# **18.2.** Hardware Signature

KeyTalk can optionally determine the state of hardware of a user's device, by calculating a hash over several components of the user's computer hardware.

The components can be chosen from the list below, and are applied in the HwSig formula as described in section 18.1 'Creating/modifying a service'.

The following component IDs are supported:

- 0 Predefined value.
- Primary HDD Serial. On Windows primary HDD is defined by minimal i for which \\.\PhysicalDrive<i> or \\.\Scsi<i> is accessible.
- 2 Primary NIC MAC-address. On Windows primary NIC is the NIC listed first in the "Network Connections" folder-> Advanced menu -> Advanced settings list.
- 3 HDDs Device Instance IDs. Only HDDS attached to IDE and SCSI are considered to avoid pluggable disks e.g. USB, PCI. Note SATA and eSATA, or PCMCIA will be used when available.
- 4 NICs Device Instance IDs. Only NICs attached to PCI are considered to avoid pluggable NICs e.g. USB.



- 5 IDE ATA/ATAPI controllers Device Instance IDs, excluding hot-pluggable one's like e.g. PCMCIA.
- 6 USB Root Hubs Device Instance IDs.
- 7 Display Adapters Device Instance IDs.
- 8 Amount of physical memory.
- 9 CPUs device instance IDs.
- 10 Interrupt controller device instance ID.
- 11 System timer device instance ID.
- 12 DMA controller device instance ID.
- 13 System speaker device instance ID.
- 14 OS Product ID.
- 15 OS registered owner.
- 16 User Security Identifier.

Some components may or may not be preferred for your setup. Choose those you need or can use. Especially in environments where users for example change local access rights, or make use of dongles, you may or may not want to enforce one or more of the above mentioned components.

In some environments it is desirable to prohibit the user to insert anything in the USB socket as this will change the HW signature of that component.



One or more authentication solutions can be connected to the KeyTalk appliance.

As a result you can use your existing infrastructure, without adding a new database.

Of course for testing purposes, or when you only have a small community, an onboard username/password database is available as well.

For example, companies with multiple branches, that manage their own authentication solution(s), such as RADIUS or LDAP/AD, can make use of a centrally available KeyTalk to turn their heterogeneous authentication environment into a funneled homogeneous authentication environment.

As a result each company may have their own preferred authentication type, but the network only needs to be configured for one X.509 certificate based solution, making the administration consistent and efficient.

By default KeyTalk has 3 authentication modules onboard. Each module can be used multiple times using its own specific configuration:

- Internal Sqlite based database
- LDAP/AD module
- RADIUS

Companies who wish to bind another type of authentication solution to KeyTalk can make use of an API, allowing an easy integration of solutions such as an Oracle Database.

# **19.1.** Internal Sqlite database module

MAIN	SERVICES	DAEMONS	UTHENTICATION M	IODULES SERS	LICENSE	CERTIFICATES AND KEYS	NETWORK	DEVICE	HIGH AVAILABILITY	LOG
alite Mod	dules   DAP N	Iodules   RADIU	S Modules   Execute N	Iodules   Relay Modu	ules					
onrigu	ure Squte A	uthenticatio	n Modules							
onfigu	ure Squte A	uthenticatio	n Modules							
onfigi	ure Squte A	luthenticatio	n Modules <sub>Servi</sub>	ce						
	ure Sqlite A	luthenticatio								

Figure 51: Configuring the Sqlite authentication modules

The Sqlite Modules section allows you to bind a <u>service</u> to a pre-configured internal database running on the KeyTalk appliance.



Typically this module is used for testing purposes or small user communities.

Though more user entries are possible, the maximum amount of users in the Sqlite should not exceed 100, if only to reduce administrative efforts.

By default the KeyTalk appliance will have the "DEMO\_SERVICE" service enabled for testing purposes. The DEMO KeyTalk client comes pre-configured with this service and the default username "DemoUser". **This database should be removed prior to taking the KeyTalk appliance into production.** 

# 19.1.1. Adding a Sqlite Module to a service

To add a Sqlite Module to a service, make certain the service exists (i.e. create it) and is not bound to another module.

Choose "ADD" and select one of the available services:

Add Sqlite Authentication Module

Service: DEMO\_SERVICE

Figure 52: adding Sqlite Authentication Module

# 19.1.2. Changing Sqlite Module settings for a service

Go to tab "AUTHENTICATION MODULES", select "Sqlite modules", select the service you would like to change and click on "CHANGE".



Figure 53: Configuring an Sqlite Authentication module



# **19.1.2.1.** HwSig Verification settings

HwSig (see section 18.2 'Hardware Signature') verification settings allow for the optional configuration of HwSig verification for the specified service.

Go to tab "AUTHENTICATION MODULES", select "Sqlite modules", select the service you would like to set the authentication to and click on "CHANGE".

MAIN	SERVICES	DAEMONS	AUTHENTICATION MODULE		LICENSE	CERT					
Sqlite Mo	odules ULDAP I	Modules   RAP	10S Modules   Execute Modules	Reby Modu	iles						
Config	Configure Sqlite Authentication Modules										
			Service								
	<b>V</b>		DEMO_SERVICE								
A	DD C	CHANGE	REMOVE								
Figure	54: Conf	iguring ar	n Sqlite Authenticatio	n modul	e						
The fo	llowing so	creen will	open:								
MAIN	SERVICES	DAEMONS	AUTHENTICATION MODULES	USERS	LICENSE	CERTIFICATES AND					
Sqlite Mo	dules   LDAP M	Modules   RADI	US Modules   Execute Modules	Relay Module	25						
	erification: Off	$\triangleright$									
		User ID		Hardware	Signature						
		DemoUser									
A	DD	CHANGE	REMOVE								
User Lo	ckout										
Automat	ically lock user o	on failed login:									
C	ж										
	User	ID	Lock Expiration		Loc	k Reason					
<b>A</b>	DD										

#### Figure 55: Configuring Sqlite Authentication module for a specific service

By default the HwSig verification is set to 'Off'.

Two other options are available for the HwSig verification:

- DevId: Obtain the user's HwId from the DevId product solution.
- Exit: Obtain the user's HwId using the settings of the authentication module.



For the option 'Exit', in the case of Sqlite Module, the HwSig is obtained from the user's Hardware Signature field.

When the 'DevId' option has been chosen, make sure that the DevId Host & Port are properly set.

#### Edit hardware signature settings for Service DEMO\_SERVICE

HwSig Verification:	DevId 💌
DevID Host:	192.168.1.2
DevID Port:	8001
DevID Group Name:	DEMO_GROUP
DevID Group Password:	•••••
ОК	CANCEL

Figure 56: Hardware signature set to 'DevId'

# NOTE:

# The HwSig verification will FAIL, thus the user is not issued a certificate when:

• The selected SERVICE is **NOT** configured to send the HwSig, and the module's HwSig Verification is set to either Exit, or DevID.

# 19.1.2.2. Add/Change/Remove user

A user can be added, changed or removed:

- Add Click on "ADD".
- Modify Select the appropriate user and click on "CHANGE".
- Delete
   Select the appropriate user(s) and click on "REMOVE".



MAIN	SERVICES	DAEMONS	AUTHEN	TICATION MODULES	USERS	LICENSE	CERTIFICATES AND
				es   Execute Modules   R			
-	erification: Of	F					
		User ID			Hardware	e Signature	
		DemoUser					
AI	DD	CHANGE		REMOVE			
Jser Lo	ckout						
Automati	cally lock user	on failed login:	<b>V</b>				
0	ĸ						
	Use	r ID		Lock Expiration		Lo	ock Reason
	DD						

Figure 57: Adding/Changing/Removing a user

Adding or changing a user, allows for entering the basic details of a user: Edit User for Service DEMO\_SERVICE

User ID:	DemoUser	
Hardware Signature:		
Password:	••••••	2
Pincode:	000000	
ОК	CANCEL	

Figure 58: Edit user for a specific user

Setting/changing the optional password of a user, requires the selecting of the password "paper-pen"-icon:

#### Edit User for Service DEMO\_SERVICE

User ID:	DemoUser
Hardware Signature:	
Password:	
Pincode:	••••••
ок	CANCEL

Figure 59: Setting/Changing a password for a user



#### Edit User password for Service DEMO\_SERVICE

User ID:	DemoUser
Enter new password:	
Re-enter new password:	
ок	CANCEL

Figure 60: Edit user password

Setting/changing the optional Pincode of a user, requires the selecting of the Pincode "paper-pen"-icon:

#### Edit User for Service DEMO\_SERVICE

User ID:	DemoUser
Hardware Signature:	
Password:	••••••
Pincode:	
ОК	CANCEL

Figure 61: Setting/Changing the pincode for a user

#### Edit User pincode for Service DEMO\_SERVICE

User ID:	DemoUser
Enter new pincode:	
Re-enter new pincode:	
ОК	CANCEL

Figure 62: Edit user pincode

#### 19.1.2.3. LockOut

The User LockOut mechanism, allows for users to be locked-out from the system when they enter the wrong authentication credentials.



#### Figure 63: enable/disable user lockout

Automatic lockout can be selected or not. Click "OK" to save the settings.

When Automatic lockout is selected, the KeyTalk appliance will add, lock and release users automatically, based on an incremental time penalty.

The Admin can always manually release users before the time penalty expires, AND can manually add or remove users to the LockOut table.



When Automatic lockout is not selected, the system runs in a manual mode, allowing the Admin to add any usernames for a permanent lock, which can only be manually released.

Adding Users manually is done using the user ID. No actual check is performed by the system to see if the User actually exists in the database used by the services' authentication module.

Lock user for Service DEMO\_SERVICE

User ID:		
ОК	CANCEL	

Figure 64: Manually adding a user to be locked out for a specific service

# 19.2. LDAP Module (Includes AD)

The LDAP module allows for Active Directories (AD) and LDAP's alike, to be easily connected to KeyTalk.

MAIN	SERVICES	DAEMONS	AUTHENTICATION M	ODULES USERS	LICENSE	CERTIFICATES AND KEYS	NETWORK	DEVICE	HIGH AVAILABILITY	LOGS
Sqlite Modules   DAP Modules   PADIUS Modules   Execute Modules   Relay Modules										
Configure LDAP Authentication Modules										
			Sar	nice						

Figure 65: LDAP Authentication Modules

ADD CHANGE REMOVE

# 19.2.1. Adding an LDAP Module

Before adding an LDAP authentication module, a new service must be defined. This service may not be connected to another Authentication Module.

Select "ADD" and select the service you wish to connect:

ES Test

#### Add LDAP Authentication Module



1

Figure 66: adding an LDAP Authentication Module

Click "OK" to save.



# **19.2.2.** Changing an LDAP Module configuration

To change an LDAP Module configuration of a service, select the appropriate service from the LDAP Configuration Module list, and select "CHANGE".

This brings up a large overview menu with several different LDAP Module configuration options:

MAIN SERVICES DAEMONS	AUTHENTICATION MODULES	USERS LICENSE	CERTIFICATES AND KEYS	NETWORK	DEVICE	HIGH AVAILABILITY	LOGS
Sqlite Modules   LDAP Modules   RADI	US Modules   Execute Modules   F	Relay Modules					
Configure LDAP Authenticati	ion Module For Service Es	5_Test					
Attribute name	Attribu	te match mode	Attrit	ute value			Filter
HWSIG		NONE	\$(	hwsig)		(sAMAc	countName=\$(userid))
HWSIG		NONE	\$(;	incode)			countName=\$(userid))
memberOf Supported placeholders: \$(service), \$		NONE					countName=\$(userid))
	URL		ind DN		P P		Server CA Certificate Exists
LDAP Server # 💷				Base DN			Server CA Certificate Exists
Server #1	ldap://localhost:389	uid=\$(userid),ou=1	lsers,dc=example,dc=com	ou=p	eople,dc=exa	imple,dc=com	
ADD CHANGE	REMOVE						
Certificate to LDAP attribute mapp	pings 🗓						
Certificate attribute LDAP attribu	ıte						
CHANGE							
User Lockout							
Automatically lock user on failed login:							
User ID	Lock Expiration	l	ock Reason				
400							

Figure 67: Configuring LDAP Authentication module for a specific service



# 19.2.2.1. HwSig Verification settings

HwSig (see section 18.2 'Hardware Signature') verification settings allow for the optional configuration of HwSig verification for the specified service.

By default the HwSig verification is set to 'Off'.

Configure LDAP Authentication Module For Service ES\_Test

HwSig Verification: Off

CHANGE

#### Figure 68: Hardware Signature verification setting

Select "CHANGE" to change the HwSig setting.

Two other options are available for the HwSig verification:

- DevId: Obtain the user's HwId from our DevId product solution.
- Exit: Obtain the user's HwId using the settings of the authentication module.

For the option 'Exit', in the case of Sqlite Module, the HwSig is obtained from the user's Hardware Signature field.

When the 'DevId' option has been chosen, make sure that the DevId Host & Port, as well as Group Name and Group password are properly set.

MAIN	SERVICES	DAEMONS	AUTHENTI	CATION MODULES	USERS	LIC
Sqlite Mo	dules (LDAP I	Modules RAD	IUS Modules	Execute Modules	Relay Modul	es

#### Edit hardware signature settings for Service ES\_Test

HwSig Verification:	Off 💌
DevID Host:	192.168.1.2
DevID Port:	8001
DevID Group Name:	DEMO_GROUP
DevID Group Password:	
ок	CANCEL

Figure 69: Editing Hardware signature settings for a specific service

#### NOTE:

The HwSig verification is considered a failed login, thus the user is not issued a certificate when:



• The selected SERVICE is **NOT** configured to send the HwSig, and the module's HwSig Verification is set to either Exit, or DevID.

# 19.2.2.2. LDAP Attribute Match Settings

To configure the LDAP attribute match settings, choose "CHANGE".

Attribute name	Attribute match mode	Attribute value	Filter				
HWSIG	NONE	\$(hwsig)	(sAMAccountName=\$(userid))				
HWSIG	NONE	\$(pincode)	(sAMAccountName=\$(userid))				
memberOf	NONE		(sAMAccountName=\$(userid))				
memberOf NONE (sAMAccountName=\$(userd)) explored placenous of \$(consin), \$(userid), \$(password), \$(pincode). Double \$ for verbatim representation of the placeholder: \$\$(password)] CHANGE							

Figure 70: LDAP attribute match settings

The following menu will open:

Edit LDAP Match Settings for Service ES\_Test

Attribute name	Attribute match mode	Attribute value	Filter			
HWSIG	NONE	\$(hwsig)	(sAMAccountName=\$(userid))			
HWSIG	NONE	\$(pincode)	(sAMAccountName=\$(userid))			
memberOf	NONE		(sAMAccountName=\$(userid))			
Supported placeholders: \$(service), \$(domain), \$(userid), \$(password), \$(hwsig), \$(pincode) 🗓						
Users with an expired password are denied access regardless of the match settings. 🗓						

OK CANCEL

Figure 71: Configuring the LDAP attribute match settings



	Attribute	Attribute matc		Attribute value	Filter
	name				
HwSig	The LDAP	none	HwSig will not be	The variable for the	Is the LDAP filter
	attribute		checked	HwSig attribute.	used to specify the
	name used	exact	HwSig needs to	-	record against which
	for storing		match exactly	Placeholders can be	the criteria are
	the	nocaseexact	HwSig must match	used for attribute	matched?
	Hardware		exactly but not	values which will be	
	Signature of		case sensitive	substituted with the	The filter may also
	the user.	subst	HwSig must be a	actual credentials	contain the following
			substring of the	provided by the	placeholders which
	Default		attribute value	KeyTalk Client.	will be substituted
	value =	nocasesubst	HwSig must be a	Supported	with the actual
	HWID		substring of the	placeholders are:	credentials provided
			attribute value but	\$(service),	by the KeyTalk
			not case sensitive	\$(domain), \$(user	Client: \$(service),
				id), \$(password),	\$(domain), \$(userid),
				\$(hwsig), \$(pincode)	\$(password),
					\$(hwsig), \$(pincode)
Pincode	The LDAP	none	Pincode will not be	The variable for the	Is the LDAP filter
	attribute		checked	Pincode attribute.	used to specify the
	name used	exact	Pincode needs to	-	record against which
	for storing		match exactly	Note: Adding a	the criteria are
	the Pincode	nocaseexact	Pincode must	separator symbol	matched?
	of the user.		match exactly but	after the variable,	
			not case sensitive	can be used to	
	Default	subst	Pincode must be a	support multiple	
	value =		substring of the	Pincode's per user.	
	HWID		attribute value		
		nocasesubst	Pincode must be a	For Example:	
		nocuscubsc	substring of the	%PinCode	
			attribute value but		
			not case sensitive		
Group	The LDAP	none	Group will not be	The variable for the	Is the LDAP filter
0.000	attribute		checked	Group attribute.	used to specify the
	name used	exact	Group needs to		record against which
	for storing	CAUCE	match exactly	Note: Adding a	the criteria are
	the Group	nocaseexact	Group must match	separator symbol	matched?
	of the user.	nocaseexact	exactly but not	after the variable can	matchea.
			case sensitive	be used to support	
	Default	cubet		multiple Groups per	
	value =	subst	Group must be a	user.	
	memberOf		substring of the		
	memberor		attribute value	For example:	
		nocasesubst	Group must be a	Admin	
			substring of the		
			attribute value but		
			not case sensitive		

# This overview explains the different fields and values:



# 19.2.2.3. Configuring LDAP module Bind & LDAPS for a service

One or multiple LDAP servers can be bound to the KeyTalk appliance. When a time-out occurs on the  $1^{st}$  LDAP, the KeyTalk appliance will try the  $2^{nd}$  etc.

To configure your LDAP module bind for your selected service: tick the LDAP server configuration entry and select "CHANGE", or select "ADD".

Configure LDAP Server connection for Service ES\_Test

JRL:	ldap://localhost:389	ii	
Bind DN:	uid=\$(userid),ou=Users,dc=example,dc=com		
Bind Password:	•••••	show	
Base DN:	ou=people,dc=example,dc=com	_	

Figure 72: Configuring LDAP Server connection

Fieldname	Description
URL	The LDAP location and appropriate port number (for Global Catalog use
	port 3268).
Bind DN	The Bind DN. Setting appropriate parameters are described in the next
	sub-chapter.
Bind Pwd	Either a bind is done using the user's credentials, or when using
	anonymous a static password can be provided.
Base DN	The Base DN

To make a secure connection possible between your LDAP/AD and KeyTalk, the LDAPS protocol is supported.

Upload the appropriate certificate using the LDAPS CA Certificate interface.

LDAPS CA Certificate (required for LDAPS only) No Certificate Found

UPLOAD

Browse...

Figure 73: Uploading a LDAPS CA Certificate

**NOTE:** The BIND DN is dependent upon the specific LDAP integration. Example: when using userPrincipalName '\$(userid)' would suffice.



# 19.2.2.4. Certificate to LDAP attribute mappings

The X.509 standard defines several fields in a certificate which must be filled in order to be RFC compliant.

By default these certificate fields are filled with the default values as set in the service. When using the default settings, your users will be provided with X.509 user certificates which are all unique based on the date/time of issuing, the serial number, and of course the username.

However, it might be prudent to have more unique user credentials in the certificate. When this is required, you can map your LDAP attributes to the certificate fields.

To map the LDAP attributes to the certificate fields: Select "CHANGE" under "Certificate to LDAP attribute mappings".

Field name	Description	LDAP attribute value
Filter	Is the LDAP filter used to specify the	Any valid value
	record against which the criteria are	
	matched?	
Country	The value of the country code as it	ISO 3166 standard value
	should occur in the user certificate.	
City/Locality	The value of the city/locality as it	Any value, except blank
	should occur in the user certificate	
Organization	The value of the organization as it	Any value, except blank
	should occur in the user certificate.	
Common Name	The value of the Users name as it	Any value, except blank
	should occur in the user certificate.	
Email	The value of the email address as it	Any value, except blank
	should occur in the user certificate.	
Time To Live	The amount of time that a certificate is	Any positive value expressed
	valid from the time it was issued.	in seconds, except blank. Can
		be 0
Time for	The default time correction factor,	Any negative value expressed
Correction	expressed in seconds, to correct	in seconds, except blank. Can
	problems when the Client system time	be 0
	is slightly off.	
		For example: -1800
Basic	The generated certificate is a user	CA:FALSE
Constraints	certificate.	
	The generated certificate is a CA	CA:TRUE
	certificate and is allowed to issue	
	certificates.	
Key Usage	Certificate Key Usage. Values should be	digitalSignature



	comma separated.	nonRepudiation
		keyEncipherment
		dataEncipherment
		keyAgreement
Extended Key	Certificate Extended Key Usage	Refer to: OpenSSL
Usage		
Subject	The value of the alternative username.	Refer to: OpenSSL
Alternative		
Name		

# 19.2.2.5. User LockOut

The User LockOut mechanism, allows for users to be locked-out from the system when they enter the wrong authentication credentials.

User Lockout	
Automatically lock user on failed login:	1
ОК	

#### Figure 74: enable/disable user lockout

Automatic lockout can be selected or not. Click "OK" to save the settings.

When Automatic lockout is selected, the KeyTalk appliance will add, lock and release users automatically, based on an incremental time penalty.

The Admin can always manually release users before the time penalty expires, AND can manually add or remove users to the LockOut table.

When Automatic lockout is not selected, the system runs in a manual mode, allowing the Admin to add any usernames for a permanent lock, which can only be manually released.

Adding Users manually is done using a free text. No actual check is performed by the system to see if the User actually exists in the database used by the services' authentication module.

#### Lock user for Service DEMO\_SERVICE

User ID:		
ок	CANCEL	

#### Figure 75: Manually adding a user to be locked out for a specific service



# 19.3.RADIUS Module

MAIN	SERVICES	DAEMONS AUTHENTICATION MODULES SERS LICENSE	CERTIFICATES AND KEYS	NETWORK	DEVICE	HIGH AVAILABILITY	LOGS	
Sqlite Mo	Sqlite Modules   LDAP Modules RADIUS Modules Execute Modules   Relay Modules							
Config	Configure RADIUS Authentication Modules							
		Service						
	DEMO_SERVICE							
AI	DO	CHANGE REMOVE						

Figure 76: RADIUS Authentication Module

When a RADIUS server is used for authentication purposes, for example when using security tokens, this module can be used to bind the RADIUS based authentication to a KeyTalk service.

#### 19.3.1. Adding a RADIUS Module

To add a RADIUS Module to a service, the service must exist and not be connected to another Authentication Module.

Select "ADD" and select the service you wish to connect: Add RADIUS Authentication Module



Figure 77: Adding a RADIUS Authentication Module

#### **19.3.2.** Changing a RADIUS Module configuration

To change a RADIUS Module configuration of a service, select the appropriate service from the RADIUS Configuration Module list, and select "CHANGE":



#### Configure RADIUS Authentication Module For Service DEMO\_SERVICE

HwSig Verification: Off						
CHANGE						
RADIUS Server #	Host	Port (0 to detect)	Max Tries	Timeout (sec)		
Server #1	localhost	0	2	2		
ADD CHANGE REMOVE						
Automatically lock user on failed login:						
OK User ID Lock Expiration Lock Reason						
ADD CHA		EMOVE				

Figure 78: Configuring the RADIUS Authentication Module for a specified service

#### **19.3.2.1.** HwSig Verification settings

HwSig (see section 18.2 'Hardware Signature') verification settings allow for the optional configuration of HwSig verification for the specified service.

By default the HwSig verification is set to 'Off'.

HwSig Verification: Off

CHANGE

Figure 79: Hardware Signature verification setting

Select "CHANGE" to change the HwSig setting.

Two other options are available for the HwSig verification:

- DevId: Obtain the user's HwId from our DevId product solution.
- Exit: Obtain the user's HwId using the settings of the authentication module.

For the option 'Exit', in the case of Sqlite Module, the HwSig is obtained from the user's Hardware Signature field.

When the 'DevId' option has been chosen, make sure that the DevId Host & Port are properly set.



#### Edit hardware signature settings for Service DEMO\_SERVICE

HwSig Verification:	DevId	-
DevID Host:	192.168.1.10	
DevID Port:	8001	
DevID Group Name:	Test	
DevID Group Password:		

Figure 80: Editing Hardware signature settings for a specific service

#### 19.3.2.2. RADIUS Server connectivity settings

	RADIUS Server #	Host	Port (0 to detect)	Max Tries	Timeout (sec)
1	Server #1	localhost	0	2	2
ADD CHANGE REMOVE					



Multiple RADIUS servers can be configured by selecting the server and clicking on "ADD". When Server #1 times out; the KeyTalk appliance will send its request to the next in line.

To change the RADIUS Server connectivity settings, select the server configuration you wish to change, and click on "CHANGE".

Fieldname	Description	Value
Host	The IP number of the Radius	Any valid IP number
Port (0 to detect)	The communication port number	Any valid port number.
		Use 0 to have the port number
		automatically detected
Secret	The Radius shared secret	Any valid Radius shared secret
Max Tries	Amount of connections attempts	Any valid positive amount up to
		999999999
Timeout (sec)	Amount of time assumed for a	Any valid positive amount
	timeout period before retrying	expressed in seconds up to
		99999999

#### 19.3.2.3. User LockOut

The User LockOut mechanism, allows for users to be locked-out from the system when they enter the wrong authentication credentials.



User Lockout

Automatically lock user on failed login:	1
--	---

ОК

#### Figure 82: enable/disable user lockout

Automatic lockout can be selected or not. Click "OK" to save the settings.

When Automatic lockout is selected, the KeyTalk appliance will add, lock and release users automatically, based on an incremental time penalty.

The Admin can always manually release users before the time penalty expires, AND can manually add or remove users to the LockOut table.

When Automatic lockout is not selected, the system runs in a manual mode, allowing the Admin to add any usernames for a permanent lock, which can only be manually released.

Adding Users manually is done using a free text. No actual check is performed by the system to see if the User actually exists in the database used by the services' authentication module.

Lock user for Service DEMO\_SERVICE

User ID:		
ОК	CANCEL	

#### Figure 83: Manually adding a user to be locked out for a specific service

# 19.4. Execute Modules



Figure 84: Executable Authentication Modules

Execute Modules are tailor made modules, officially released by KeyTalk BV as NON-STANDARD. These modules are not part of the formal firmware release.

Though it is not the policy to release modules outside of the officially supported firmware releases, this feature allows for it to be made possible when executing beyond policy.



Licensing restrictions may apply. Consult your KeyTalk supplier or partner for more information.

# **19.5.** Relay Modules (connecting other authentication solutions)



Figure 85: Relay Authentication Modules

Relay Modules, allow you to make use of the REMAP API, to connect to authentication solutions which are not by default supported by KeyTalk. REMAP: KeyTalk Exit Module Authentication Protocol.

Customers and partners of KeyTalk have made available some unsupported API implementations, which can be requested through your KeyTalk supplier or partner.

#### 19.5.1. Adding a Relay Module

To add a Relay Module to a service, the service must already exist and not be connected to another Authentication Module.

Select "ADD" and select the service you wish to connect: Add Relay Authentication Module

Service: DEMO\_SERVICE

ОК

Figure 86: Adding a Relay Authentication Module

# 19.5.2. Changing the Relay Module service configuration

To change the configuration settings, select the Relay Module service for which you wish to change the configuration, and select "CHANGE".



**Configure Relay Authentication Modules** 

	Service
<b>V</b>	DEMO_SERVICE
ADD	CHANGE REMOVE

#### Figure 87: Configuring the Relay Authentication Module for a specified service

You will now see the current configuration, which can be changed by selecting "CHANGE".

#### Configure Relay Authentication Module For Service DEMO\_SERVICE

Remote Host:	backauth.reseptdemo.com
Remote Port:	9001
Use TLS:	$\checkmark$
Server Communication Key Signer CA Exists:	

CHANGE

Figure 88: Current configuration

#### Edit Relay Authentication Module for Service DEMO\_SERVICE

Remote Host:	backauth.reseptdemo.com				
Remote Port:	9001				
Use TLS:					
ОК	CANCEL				

Figure 89: Editing the configuration

Since the Relay module effectively makes use of a host running remote, only a connection needs to be defined for the Remote Host.

Configure the Remote Host and corresponding Port and whether or not TLS should be used to secure the communication.



#### Figure 90: For TLS a server communication key signer CA certificate is needed

Additionally when using SSL/TLS you will need to upload the Server Communication Key Signer CA certificate in PEM format. This does NOT need to be a certificate created under your Certificate Authority tree, but can also be that of a 3<sup>rd</sup> party, such as VeriSign, or Microsoft.



# 19.5.3. Remote exit basics

When you wish to create your own authentication module (exit), you should always run it from a separate server.

The details of what needs to be configured are covered in a separate Remote Exit document which is available through your KeyTalk supplier or partner.

# **19.6.** Synchronize User Lockout List

MAIN	SERVICES	CONFIGURE DAEMONS	AUTHENTICATION MODULES	USER MESSAGES	LICENSE AND KEYS	NETWORK	DEVICE	LOGS	
Sqlite Mo	dules   LDAP	Modules   RADIUS Modules	Execute Modules   Relay Modu	les Cynchronize Us	er Lockout List				
Manua	lly Synchro	nize User Lockout Lis	t Accross Chains						
			est configured chains each time erver chains. Click "Copy" to cop					ou may n	eed to force manual
Note: Be	fore copying (	please make sure <u>DbServi</u>	ce connection address points to	the chain's had.					
<b>CO</b>	PY								

#### Figure 91: Synchronize user lockout list

This functionality is only applicable when running KeyTalk in a high availability configuration.

This feature allows you to manually initialize a synchronization of all your User Lockout Lists from all your Authentication Modules for all services on the KeyTalk appliance.

HA will automatically synchronize, but the manual feature is meant for synchronization after adding a new system to your High Availability setup.



### 20.1. User messages

User messages allow the Organization's administrator to send a custom message to the user when their KeyTalk client starts.

A common usage would be to inform users of network downtime announcements for example.

To create a user message, select "USERS" from the main menu and click on "ADD".



Figure 92: Adding a user message

Type the message that needs to be sent to all users with a KeyTalk Client and click "OK" to make the message available to your user community.

User Message:	*
,	~

Figure 93: Adding user message and making it available to the KeyTalk Client users

An existing user message can be changed or removed by selecting the user message and clicking on "CHANGE" or "REMOVE".

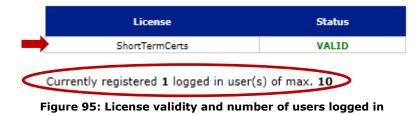


Figure 94: Changing or removing a user message



# 20.2. Logged-in Users

You can check if your license is still valid. Additionally, your license to serve a number of users can also be checked per service on the "MAIN" tab of KeyTalk.



It is possible that some users have left your company, but are still counted as 'logged in users'. To correct the user-counter field the "RESET" button on the "USERS" tab can be clicked, deleting the 10% of users that did not log in recently (oldest first).

	MAIN	SERVICES	DAEMONS	AUTHENTIC	ATION MODULES	USERS	LICENSE	CERTIFICATES	AND KEYS	NETWORK	DEVICE	HIGH AVAILA	BILITY	LOGS	
	Logged-I	n Users   User	Messages												
	Currentl	y registered	1 logged in u	ser(s) of max	. 10										
<	RE	SET i	>												
		Ser	rvice		User			Last Login					Client Ve	ersion	
		DEMO_	SERVICE		DemoUser			10-07-2012 14:	03			RESEP	T Regular	Client-4.2	.0
	Page 1	💌 of 1 U	sers per page	e: 50 💌											

Figure 96: Resetting the oldest 10% of counted users

Deleting this 10% of oldest counted users can also be done via the LCD menu. See section 24 'LCD information display' for more information.



# 21. KeyTalk Appliance License

The KeyTalk Appliance License file contains the general terms & conditions text in a text file format. Your contract details override or amend these T&C. It is personalized to your company and contains all the information required to make the appliance work.

DAEMONS AUTHENTICATION MODULES USERS LICENSE CERTIFICATES / SERVICES MAIN License Info Function: ShortTermCerts Allowed: ves Expires: 2014-01-01 Max Users: 10 Upload License Browse... UPLOAD

Your license details can be viewed under the "License" tab.

Figure 97: View license info or upload a new license

A new license can be uploaded by selecting the license via "Browse..." and clicking "UPLOAD".

The text file is signed by KeyTalk, ensuring that any tampered text files cannot be uploaded as a valid license. The maximum amount of users refers to the maximum amount of unique usernames used to obtain a certificate in a given timeframe.



# 22. Certificates and keys

On the "CERTIFICATE AND KEYS" tab the Certificate Authority Keys for the KeyTalk appliance can be managed.

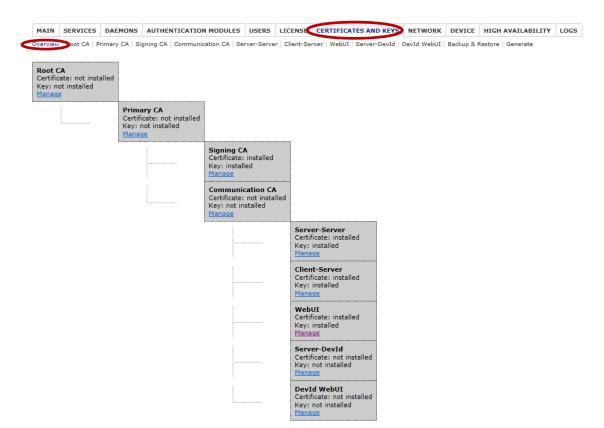


Figure 98: Overview of the KeyTalk Certificate Authority Keys

By default your KeyTalk appliance comes pre-configured with test key and certificate material. This material is NOT unique, but provided with every system. It is therefore necessary to be replaced by your own material when going into production.

KeyTalk requires the certificates to be imported or generated in PEM file format and requires that they contain the .pem file extension.

Please note that the KeyTalk solution does not mandatorily require you to take into account any specific protocols and procedures as to the security level of key-creation, key management, etc. Instead it is your company who decides what is and what is not acceptable.



# 22.1. Root CA

The Root CA is an optional public certificate. It is only applicable when your company already has an existing certificate authority in place.

When installed it may serve as a root for the certificate tree generated on the appliance.



Figure 99: Root CA information and key upload functionality

A new certificate can be uploaded by selecting it via "Browse..." and clicking "UPLOAD".

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.

### 22.2. Primary CA

The Primary CA is a private key and is normally a root of the certificate tree unless the Root CA is installed and is an issuer for the Primary CA.

After generation this key is kept offline and is usually stored on a portable media in your safe. Depending on your security requirements it can be distributed in parts, for safe keeping, among several custodians.

This file also contains the Primary CA Certificate in PEM format.



Figure 100: Primary CA information and key upload functionality

A new certificate can be uploaded by selecting it via "Browse..." and clicking "UPLOAD".



After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.

# 22.3. Signing CA

This tab allows you to upload your own signing certificate and key, used to issue user certificates and keys. When you have a separate key and certificate you can upload these individually and KeyTalk will combine them for you.

MAIN	SERVICES	DAEMONS	AUTHENTICATION MODULES	USERS	LICENSE CER	TIFICATES AND KEYS	PETWORK	DEVICE	HIGH AVAILABILITY	LOGS	
verview	Root CA   F	Primary C/	gning CA Pommunication CA   Se	rver-Serve	r   Client-Server	WebUI   Server-DevId	DevId WebUI	Backup &	Restore   Generate		
ionina (	TA is used b	v CAD to sign	generated certificates, RESEPT	conver re	quires both certil	icate and key DESEDT	client only n	aquiras car	tificate (UCA) which is in	ncluded i	n PCCD fi
		y CAD to sign	generated certificates. RESEPT	server re	quires both certi	icate and key. RESEPT	client only h	equires cer	uncate (OCA) which is it	nciudeu i	II KCCD II
Certific	ate Info										
Subject:		C=NL ST=Utrech	t L=Soesterberg O=Resept Demo OU=	Demo Only	CN=Resept Demo S	gning CA emailAddress=der	mo@reseptdem	o.com			
Issuer:		C=NL ST=Utrech	t L=Soesterberg O=Resept Demo OU=	Demo Only	CN=Resept Demo P	CA emailAddress=demo@re	septdemo.com				
Valid From	n: :	22-03-2011 13:2	5 ( 22-03-2011 13:25 GMT )								
Valid To:		17-05-2027 13:2	5 ( 17-05-2027 13:25 GMT )								
Signature	Algorithm: s	sha1WithRSAEnc	ryption								
Public Key	r I	RSA (4096 bits)									
5HA1 Fing	gerprint:	1ab4f901faedd76	if9f10a9cd5ced9744af218420								
Jpload		e and Key	taining certificate and key. The	key should	d not be protecte	d with password. It is a	also possible	for the PEN	1 file to contain certifica	te or key	only.
		cate and Ke									
Click "Do	ownload" to	download cer	tificate and key as a single PEM	file.							
DOWN											
2011010	e Certifica	te and Key									
REM											

#### Figure 101: Signing CA information and key upload functionality

This screen allows you to download and remove the current certificate and key, and upload a new version.

A new certificate can be uploaded by selecting it via "Browse..." and clicking "UPLOAD".

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.



# 22.4. Communication CA

This tab is used to secure communications between different parts of the system. The Communication CA corresponds to the SCA (Server CA) on the client-side.



#### Figure 102: Communication CA information and key upload functionality

A new certificate can be uploaded by selecting it via "Browse..." and clicking "UPLOAD".

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.

# 22.5. Server-Server Communication Key

This tab allows you to view the information of the Server-Server Communication Key and certificate.

This certificate and key is required to encrypt the information exchange between KeyTalk servers in High Availability mode; and to encrypt the information exchange between KeyTalk and the DevID additional module.

You can upload the combined certificate and key as a single file or you can upload the key and the certificate as separate files in PEM format. There is no need to rename the files, as KeyTalk will do this for you.



MAIN SERVICES DAEMONS AUTHENTICATION MODULES USERS LICENSE CERTIFICATES AND KEYS ETWORK DEVICE HIGH AVAILABILITY LOGS
Overview | Root CA | Primary CA | Signing CA | Communication CA Server-Serves Client-Server | WebUI | Server-Devid | Devid WebUI | Backup & Restore | Generate

Server-server certificate and key are used to secure communication between RESEPT servers in High Availability setup.

Certificate Info	
------------------	--

Subject:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=localhost.reseptdemo.com emailAddress=demo@reseptdemo.com
Issuer:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=Resept Demo CCA emailAddress=demo@reseptdemo.com
Valid From:	22-03-2011 13:32 ( 22-03-2011 13:32 GMT )
Valid To:	17-05-2027 13:32 ( 17-05-2027 13:32 GMT )
Signature Algorithm:	sha1WithRSAEncryption
Public Key:	R5A (2048 bits)
SHA1 Fingerprint:	ea155ebbd9e18792af81c6e5aaf1c804f765007c

Key Info

Type: RSA (2048 bits)

#### Upload Certificate and Key

Click "Upload" to upload PEM containing certificate and key. The key should not be protected with password. It is also possible for the PEM file to contain certificate or key only.

Browse
Download Certificate and Key
Click "Download" to download certificate and key as a single PEM file.

DOWNLOAD
Remove
REMOVE

#### Figure 103: Server-server certificate information and key upload functionality

This screen allows you to download and remove the current certificate and key, and upload a new version.

A new certificate can be uploaded by selecting it via "Browse..." and clicking "UPLOAD".

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.

# 22.6. Client-Server Communication Key

This tab allows you to view the information of the KeyTalk Client-Server Key and certificate.

This certificate and key is required to establish a secure connection between the KeyTalk client and the KeyTalk server.

You can upload the combined certificate and key as a single file or you can upload the key and the certificate as separate files in PEM format. There is no need to rename the files, as KeyTalk will do this for you.



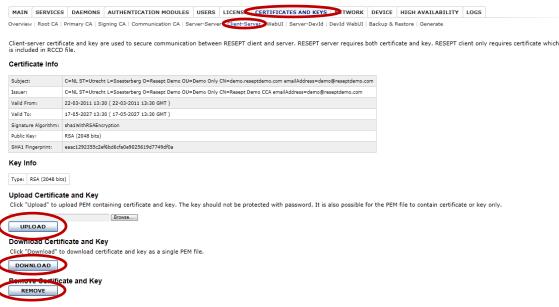


Figure 104: Client-server certificate information and key upload functionality

This screen allows you to download and remove the current certificate and key, and upload a new version.

A new certificate can be uploaded by selecting it via "Browse..." and clicking "UPLOAD".

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.

# 22.7. WebUI Certificate & Key

This tab allows you to view the information of the KeyTalk Admin Graphical User Interface.

It is used to secure the communication between the KeyTalk appliance and the computer of the organization's administrator (single SSL). You should choose to purchase this certificate ad key from a 3<sup>rd</sup> party certificate provider. For more information please refer to section 8.1 'Replacing Admin GUI SSL-certificate'.

A separate WebUI key and certificate are required for each KeyTalk and DevID appliance, since each appliance will run under its own unique FQDN in the network.





WebUI certificate and key are used to secure access to the RESEPT server UI via browser.

Certificate Info	
Subject:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=reseptadmin.reseptdemo.com emailAddress=demo@reseptdemo.co
Issuer:	C=NL ST=Utrecht L=Soesterberg O=Resept Demo OU=Demo Only CN=Resept Demo CCA emailAddress=demo@reseptdemo.com
Valid From:	22-03-2011 13:34 ( 22-03-2011 13:34 GMT )
Valid To:	17-05-2027 13:34 ( 17-05-2027 13:34 GMT )
Signature Algorithm:	sha1WithRSAEncryption
Public Key:	RSA (2048 bits)
SHA1 Fingerprint:	24339f015e2cf046a7ba95ef0c1df5fe7af9045a
Upload Certifica Click "Upload" to u	<b>te and Key</b> pload PEM containing certificate and key. The key should not be protected with password.
UPLOAD	Erowse
Download Certi	ficate and Key
Click "Download" t	o download certificate and key as a single PEM file.
DOWNLOAD	

Figure 105: WebUI certificate information and key upload functionality

This screen allows you to download the current certificate and key, and upload a new version.

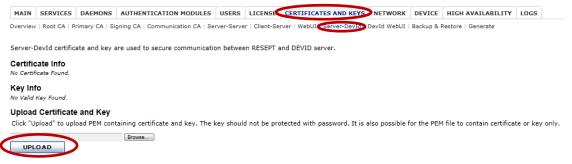
A new certificate can be uploaded by selecting it via "Browse..." and clicking "UPLOAD".

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.

# 22.8. Server-DevID Certificate & Key

The Server-DevID certificate and key is used to secure communication between the KeyTalk Server and the DevID appliance.



### Figure 106: Server-DevID certificate information and key upload functionality

A new certificate can be uploaded by selecting it via "Browse..." and clicking "UPLOAD".



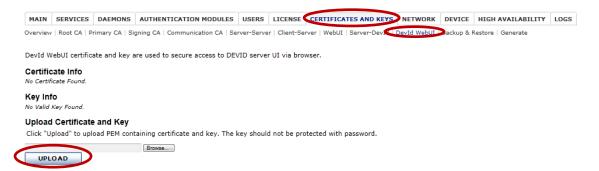
After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.

# 22.9. DevID WebUI Certificate & Key

The DevID WebUI certificate and key are used to secure access to the DevID server UI via a browser.

A separate DevID WebUI key and certificate are required for each DevID appliance, since each one will run under its own unique FQDN in the network.



#### Figure 107: DevID WebUI certificate information and key upload functionality

A new certificate can be uploaded by selecting it via "Browse..." and clicking "UPLOAD".

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.

# 22.10. Backup & Restore

This tab allows you to make a full backup of your current certificates and keys, as well as granting the ability to restore your backup, if required.





ALL currently installed certificate/keys will be removed during restoration. The device management interface may automatically restart after the certificates/keys package is restored.

#### Figure 108: Backup and restore functionality

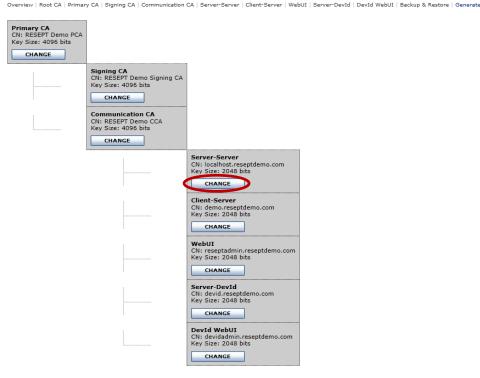
Click "Backup" to save all currently installed certificates and keys to your computer.

Click "Restore" to restore all certificates and keys from the previously made backup. The KeyTalk appliance will reboot afterwards, to effectuate the changes.

### 22.11. Generate

This tab allows you to edit specific criteria for the certificates that have been generated on the appliance.

MAIN SERVICES DAEMONS AUTHENTICATION MODULES USERS LICENSE CERTIFICATES AND KEYS NETWORK DEVICE HIGH AVAILABILITY LOGS



📃 Include Root CA 🚺

Click "Generate Tree" to generate a certificate tree using the configuration specified on this page. When done you will be prompted to install the generated certificates to the appliance.

GENERATE TREE

Figure 109: Edit specific criteria for all hosted certificates



Click on `CHANGE' to edit a specific set of certificate fields. Click `OK' to accept the alterations.

MAIN	SERVICES	DAEMONS	AUTHENTICATION MODULES	USERS	LICENSE	CERTIFICATES AND KEYS	NE
Overview	Root CA   P	rimary CA   Sig	gning CA   Communication CA   Se	rver-Serve	r   Client-Se	rver   WebUI   Server-DevId   [	DevI

#### Edit Client-Server certificate fields

Common Name:	demo.reseptdemo.com
RSA Key Size (bits):	2048 💌
Country:	AC 💌
City/Locality:	
Organization:	
Organizational Unit:	
Email:	
Time To Live (sec):	315360000
Time For Correction (sec):	-3600

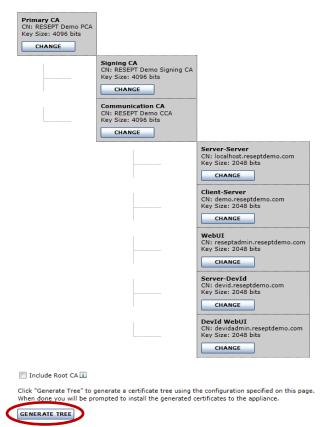
### Figure 110: Edit specific Client-Server certificate fields

Once you have finished editing the necessary certificate fields; you are ready to generate the newly configured certificate tree.



 MAIN
 SERVICES
 DAEMONS
 AUTHENTICATION MODULES
 USERS
 LICENSE
 CERTIFICATES AND KEYS
 NETWORK
 DEVICE
 HIGH AVAILABILITY
 LOGS

 Overview
 Root CA
 Primary CA
 Signing CA
 Communication CA
 Server-Server
 VebUI
 Server-DevId
 DevId WebUI
 Backup & Restore
 Generate



#### Figure 111: Generate the newly configured tree

Click "Generate Tree" to generate a certificate tree using the configuration specified on this page. When done you will be prompted to install the generated certificates to the appliance.



#### Figure 112: Install the generated certificate tree

After a successful UPLOAD the device management subsystem will automatically restart to effectuate the new certificate tree.

To make the changes permanent, please refer to section 8.2 'Saving changes & reboot'.



# 23. Errors and error-reporting

KeyTalk 4.x provides error messages.

- These messages are:
- Resolved IP invalid
- Digest Invalid
- Time out of sync
- Server error

#### When an error cannot be resolved, the Admin should run "Report Problem" function.

 MAIN
 SERVICES
 DAEMONS
 AUTHENTICATION MODULES
 USERS
 LICENSE
 CERTIFICATES AND KEYS
 NETWOR
 DEVICE
 HIGH AVAILABILITY
 LOGS

 Time
 Admin Password
 SSH Access
 Save & Reset Configuration
 Backup & Restore Configuration
 Firmware Upgrade
 Shut Dow
 Report Problem

 Report Problem

 Encounter a problem? Please help us solve it by following the steps below.

 Step 1. Click "Save" to generate the recent device activity report and save it to a file.

 Step 2. Send the saved report file along with the problem description to your RESEPT support contact.

#### Figure 113: Generate a problem activity report

Save the resulting file, and send it to your KeyTalk supplier or partner with a written description of the problem, preferably substantiated with screenshots, repro steps and log files.



Front Panel component 'J' provides information to those accessing the physical KeyTalk appliance.

Using buttons A, B, C and D, allows you to navigate the different information screens on the LED display.

Normal mode				Direct code mode				
Button	А	В	С	D	Button	А	В	С
Effect	Back	Up	Down	Confirm	Effect	Position 1: 0-9	Position 2: 0-9	Position 3: 0-9

To activate the LCD information display menu, touch any of the buttons A, B, C or D. After it has been activated you can press 'D' to activate the Direct Code mode. Press buttons A-C to go to the Normal mode.

Select and confirm any of the three figure menu items will make the LCD go to its default display.

Menu item		m					
		Direct code	Description	Effect			
0			Direct code	Activate direct code			
1			Device	Go to device sub-menu			
	11		Power	Go to the power sub-menu			
		111	Reboot	Reboot the appliance. This will make the active configurations persistent.			
	12		IP reset	Go to IP reset sub-menu			
		121	External	Reset the external IP to default (perform 131 manually)			
		122	Internal	Reset the internal IP to default (perform 131 manually)			
		123	Management	Reset the management IP to default (perform 131 manually)			
	13		Maintenance	Go to the KeyTalk maintenance sub-menu			
		131	Reset users	Reset the oldest 10% of the user license count			
		132	Save Settings	Save changed settings			
		133	Reset Settings	Reset all appliance settings to factory default and reboot			
		134	Upgrade	Activate the FWUPGRADE			
2			Info	Go to the information sub-menu			
	21		KeyTalk	Go to the KeyTalk information sub-menu			
		211	Version	Display the current KeyTalk appliance firmware version			
		212	Counted users	Display counted users for license purposes			
	22		IP Address	Go to the IP information sub-menu			
		221	External	Display the current external IP number			
		222	Internal	Display the current internal IP number			
		223	Management	Display the current management IP number			



D

Confirm

# 25.1. KeyTalk Appliance firmware

Version	Release date	Description
4.0.0	June 1st 2011	Initial release
4.1	January 23rd 2012	Significant efficiency improvement, upgraded OS, upload firmware option, added DevID module support, updated HAD functionality, download & remove functions on daemon certificates & keys, total unique users per service reporting, LCD based oldest unique user cleaning (max 10%)
4.2	July 2012	Update documentation to KeyTalk 4.2. In 4.2 it is possible to generate the CA tree on the appliance.



# 26. Manufacturer information

Manufacturer:	KeyTalk BV				
	Nijverheidsweg Noord 78				
	3812 PM Amersfoort The Netherlands				
	Telephone:	+31 64 672 67 94			
	Fax:	+31 84 875 43 37			
Email:	<u>info@keytal</u>	<u>k.com</u>			
Web:	www.keytalk.com				
	Chamber of Commerce: 57420858				
	VAT Number: NL852572955B01				
Bank:	Rabobank				
	Bank	NL14 RABO 0132 1619 15			
	BIC	RABONL2U			
	RESEPT, Tru	ustAlert and KeyTalk are a brand of KeyTalk BV			



# Index

# G

Getting	started8
cecting	otal tealling of the second seco

# I

Installation	.9
Introduction	.7

# S

Support	9
System configurations	9

# U

Using the software .....9

