iOS app

User manual

Company	KeyTalk IT Security BV
Author	MR van der Sman
Creation date	6 July 2018
Last updated	22 May 2019
Product	KeyTalk iOS app
Data classification	Public
Software version	5.5.6
Manual version	5.5.6.1

Contents

1. Introduction

KeyTalk for iOS securely sends your authentication details to your corporate KeyTalk server instance, protecting your authentication details against malicious Man-in-the-Middle intrusions.

The KeyTalk app will additionally identify your device as a trusted device belonging to you. KeyTalk does this based on a hash of your device components and software characteristics.

Upon your positive authentication, KeyTalk for iOS will install with your help, proof of your identity on your iOS device. This proof of identity is known as an X.509 certificate which comes with a unique and strong encryption key-pair.

With this proof of identity, your iOS device is enabled for S/MIME based secure email encryption and can use the same proof of identity to establish a secure connection to a target corporate server or VPN, in order for you to exchange your privacy and corporate sensitive data to the target network.

2. How to

Step 1: Download the KeyTalk for iOS app

Your company will either deploy the app by means of a Mobile Device Management solution,

or

you can download the KeyTalk for iOS app from the Apple App Store: search for KeyTalk 5

Step 2: Configure the KeyTalk for iOS app

When your company has deployed the app by means of a Mobile Device Management solution its very likely already configured and you don't need to undertake any configuration steps.

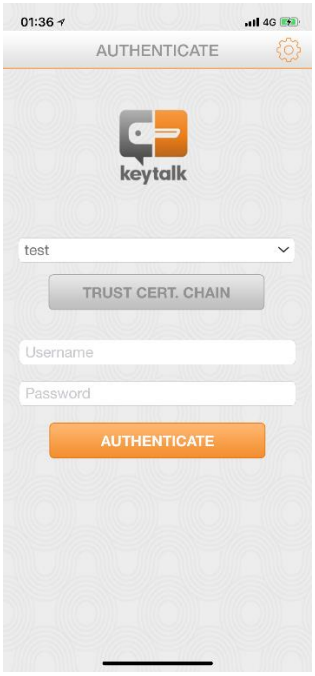
Should you have installed the KeyTalk app yourself from the App Store, then you will need to configure the app using a KeyTalk Real Client Configuration Data file (RCCD).
You will either have received this RCCD file in an email from your company or service provider, or may have received a link or url to it.

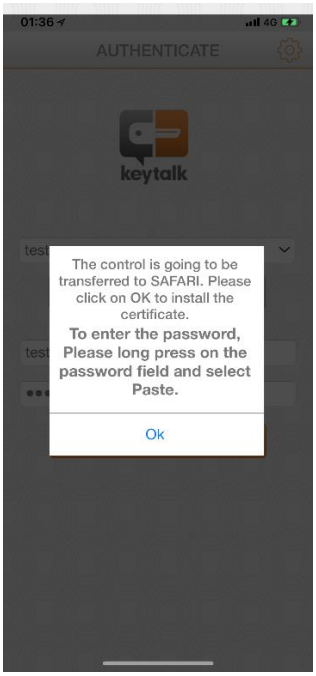
When you received it as an attachment, simply open the attachment and it will be imported into your KeyTalk client.
When you received a link/URL, just copy the link/URL in the app's settings menu:

Step 3: Request your proof of identity / certificate

From the main app screen select the service you would like to use.
It's possible that multiple services may exist, for example authentication and email encryption.

When multiple options exists, simply choose 1, authenticate using your corporate authentication credentials, and repeat the steps for the other services you may wish to make use of.

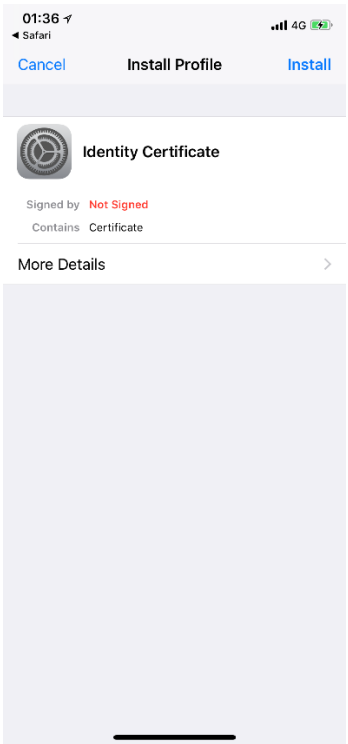


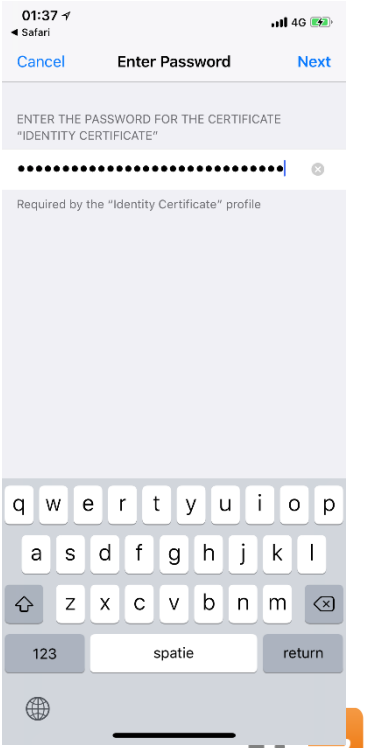


Step 4: Install the proof of identity / certificate

Provided your authentication was positive, through Safari you will be offered a certificate.
This certificate needs to be installed which requires your input to enable it device wide.

Allow the configuration profile -> select install -> paste the password (it's stored already in memory)





3. Other settings explained

From the setting menu the following additional options exist:

IMPORT: Effectuates the import of the config file from the entered url

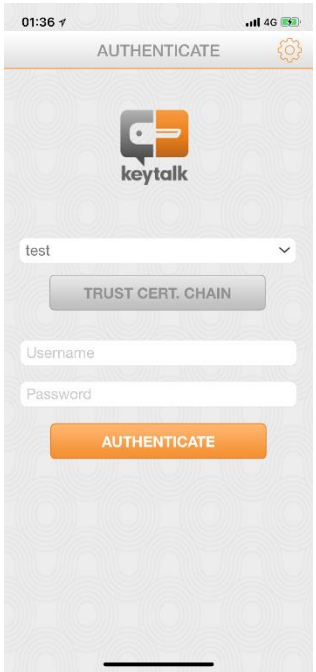
Language: Change app language

App Unlock: Enables iOS device security code to open the app

SEND REPORT: Create and send a Problem Report to your support Department or service provider

REMOVE CONF: Removed all configuration settings

TRUST CERT CHAIN: Enables the download and subsequent installation of your company's corporate KeyTalk private CA. Only needed when using KeyTalk private CA certificates



4. FAQ

Question 1: Where in iOS can I find my installed certificates and keys?
Answer 1: The KeyTalk based issued certificates are installed in the iOS certificate chain
It can be found under: settings -> general -> profiles

Question 2: Where in iOS do I set my email encryption?
Answer 2: Set your applicable S/MIME encryption certificate under:
Settings -> Accounts&Passwords -> your mail account -> account -> Advanced Settings -> S/MIME

Question 3: Can certificates and keys also be sent to an iOS device without the KeyTalk app?
Answer 3: Yes, KeyTalk is releasing support for commonly used Mobile Device Management (MDM) solution support, as of Q3 2019

Question 4: My credentials are supposedly wrong, what's causing this problem?
Answer 4: The KeyTalk server verifies the entered authentication credentials against a used Identity Provider Solution, such as Active Directory or MySQL etc. When these are correct, an additional trusted device verification is made, ie does your used device belong to you according to the company offering the KeyTalk Certificate Life Cycle Management solution.
So it's very likely that when your username/password are correct, that your device is not being trusted. Kindly contact your KeyTalk service provider support department to resolve this problem.

5. About KeyTalk

KeyTalk IT Security is a certificate & key and enrollment software solution manufacturer.

It's registered with the Dutch chamber of commerce under: 59072555
with registered VAT number: NL853305766B01

Our office visiting address:
Kleine Haag 21a
3811HE Amersfoort
The Netherlands

Website: https://www.keytalk.com
Firmware/software: https://www.keytalk.com/download

Should you encounter any issues with the app, please generate a Problem Report using the app's inbuilt PR generator feature (see chapter 3) and submit the problem report to your KeyTalk service provider, or your IT department.