TELETASK

trendsetter in domotics

INTERNET SAFETY

HOW SAFE IS IT TO CONTROL YOUR HOUSE/ BUILDING OVER THE INTERNET?

No software protection offers a 100% guarantee. However, you can take some security measures to prevent your data from falling into the wrong hands. Therefore, TELETASK always uses at least TLS encryption (embedded in our TT Cloud connections) to provide a very high level of security.

TLS ENCRYPTION

At TELETASK, a complete security package consists of different techniques. The primary security layer is combined with a TLS protected connection that makes it possible almost completely to avoid unwanted entries.

What does an encrypted TLS connection do? TLS not only encrypts data but also verifies each connection to ensure a high level of security.

TELETASK systems use a wired bus network in your home. A wired solution is often not only more robust but also easier to secure. Moreover, there is only one soft link to the Internet, which is always at least encrypted with TLS. That's where the difference with an IoT network is. In such a network, each sensor or actor is individually connected to the cloud, significantly increasing the risk of unwanted access. That's why TELETASK takes a different approach.

Your TELETASK connection uses a wired bus and Ethernet cable network. That's why your system integrator can guarantee added security levels. At any time, at any level.

Don't forget that third parties can enter your home not only electronically but also in a simple mechanical way. If you want to protect yourself against unwanted access to your home, you also need to use proper gates, doors, windows, roof, glass, and locks. Throwing a stone through a window may be easier for a burglar to access your property than hacking into a TLS secured connection.

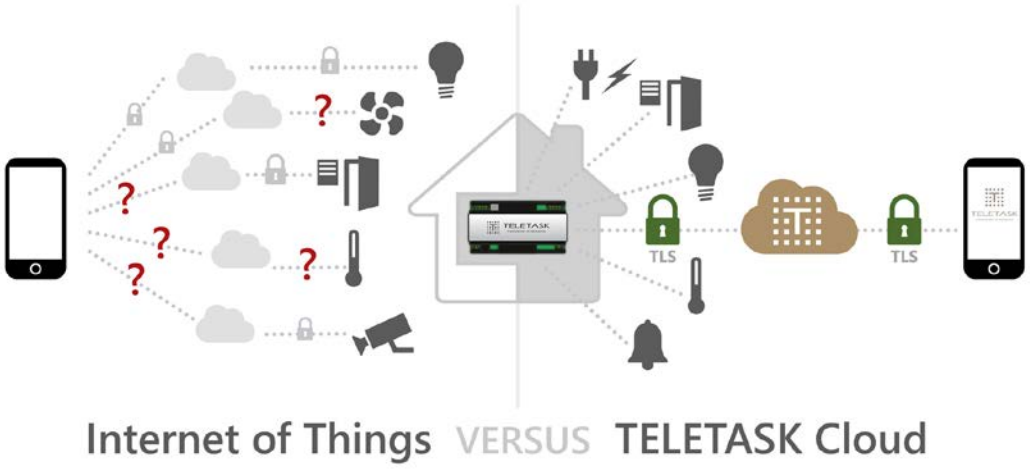
TTCLOUD CONNECTIONS

TELETALK's cloud connections (TTCloud) are also always protected by TLS. TTCloud is used to remotely control smart homes and buildings, whether or not via an application on your smartphone, desktop, or tablet. This means you are also optimally protected outside your home network. No additional security actions are needed for residential and professional applications.

TTCloud allows users to connect to the TELETASK app from anywhere in the world to monitor and control their home automation applications. In addition, the system integrator can remotely maintain and upgrade all TELETASK applications via the secure "Remote Services".

TELETASK

trendsetter in domotics



LOCAL SETUP

At TELETASK, you can also communicate only locally (in your home or building). In this case, your system is not connected to the cloud and only works via your local network. This way, you retain 100% control over the integrated devices and systems without connecting to the outside world.

You cannot remotely control your smart home installation if you work with a local setup. That's why almost every customer uses the standard fully secure smartphone app TELETASK offers.

VPN

Thanks to TLS encryption, it is no longer necessary to use a VPN connection. If you still want to set up your own cloud connection, you can do this in two ways:

1. You can configure your router to work with port forwarding. However, this offers NO SECURITY! Therefore, TELETASK strongly disapproves of this method.

2. You can configure your router to work with VPN tunnelling: this also offers a high level of security, just like TTcloud above.

So if you do want to use a VPN connection, TELETASK strongly recommends that you choose a secure VPN. Definitely do not use port forwarding. The responsibility lies entirely with the system integrator who sets up these connections.

EXTRA TIPS

1. Ensure that the TELETASK central unit and its LAN access are installed in the secure zone of your project (security system protected area). The system integrator should ensure that it is impossible to disable the security system remotely.

2. The "remote management" feature of your router (WAN side) should be disabled (most routers have this pre-programmed by default).

3. If you use Wi-Fi, use at least WPA/PSK or higher.

4. When leaving the house or building, it is best to automatically switch off all Wi-Fi routers. This can be done very quickly with the TELETASK system. You can also shut down all Wi-Fi routers automatically after or during a specific period of time (night) by turning off the router's power supply.

5. Do not provide publicly accessible Ethernet wall sockets connected to the secure LAN in public areas.

6. External technical support personnel may have access to the secured zones (e.g., lift maintenance personnel...). However, make sure they do not have access to your secure LAN.

7. Always use good passwords (minimum eight characters long, minimum one capital letter, and one number). Do not repeat your passwords, and preferably use password management software.

www.teletask.be