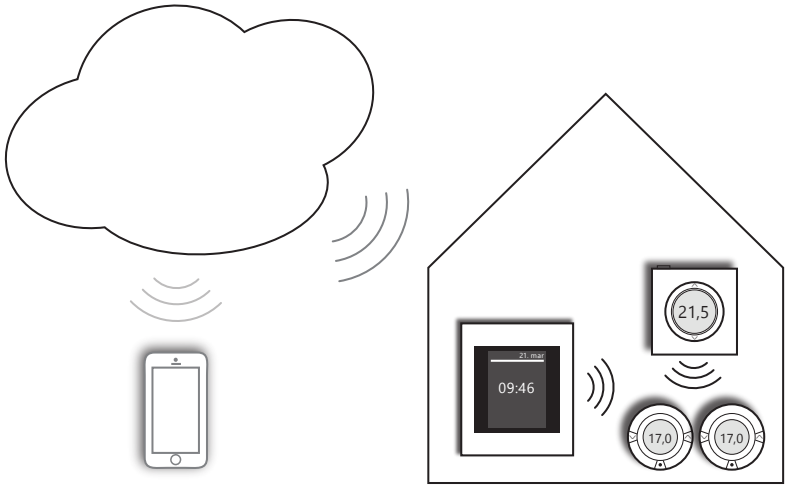
ENGINEERING
TOMORROW

Technical Paper

Danfoss Link™ Data Security

Background



Danfoss Link™ consists of three main parts:
- Z-Wave components (in the house)
- Link™ to Cloud server (house to internet)
- Cloud server to App (internet)

In the house - wireless Z-Wave:
- **Usage:** Z Wave networks wireless transmit temperatures, set points and heating notifications between thermostats, room sensors and the Link™ panel
- **Security:** Data is transmitted using secure proprietary protocols.

Out of house – Link™ to Cloud server:
- **Usage:** Only data requested, eg temperature in a room is sent out to the cloud and onwards to the requesting App.
- **Security:** Wifi connection from Link™ to router using WPA2 encryption. Link™ to Cloud server is also encrypted using AES encryption and is very secure.

Cloud server to App:
- **Usage:** Sending requested data to the App or requesting data from the Cloud server
- **Security:** Cloud server to App is also encrypted using AES encryption.

Secure

Securing against threats:
Hacking into the Cloud server or Link™ is protected through AES encryption.
Further to verify that it is indeed a strong protection the security is tested yearly through independent data security specialists trying to hack into the system*. In addition code review is conducted continuously to verify that no back doors exists.

Data protection:
To further ensure the data privacy user data such as temperatures or set points is only stored in the cloud, if you give your consent. Please see valid End User License Agreement.

System integrity:
The *Danfoss Link*™ system is not connected to non Danfoss systems and hence is not weakened by other parties.

Physical protection:
A pin code features ensures that only the administrator can operate the Link™

Several tests are performed to hack into the *Danfoss Link*™ system including but not limited to:
- Denial of service attack (DOS)
- Injection + port scan
- Missing function level access control
- Security misconfiguration
- Sensitive data exposure

**The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. Source Techtarget*

How to communicate

Aiming to secure highest possible data security level.

- Data in the cloud is protected through the encryption standard used by the U.S. government to protect classified information.
- System is tested yearly through independent data security specialists.
- A pin code feature ensures that only the administrator can operate Link™
- User data such as temperatures or set points is only stored in the cloud, if you give your consent. Please see valid End User License Agreement.

Danfoss A/S
Heating Segment • heating.danfoss.com • +45 7488 2222 • E-Mail: heating@danfoss.com