Written by Marco Attard
25 November 2016

The Z-Wave Alliance adds a further security requirement to the Z-Wave certification-- the new Security 2 (S2) framework requires the adoption of strongest levels of IoT security in the industry.

According to the alliance, the S2 framework provides the most advanced security for smart home devices and controllers, gateways and hubs, and will be mandatory for all products receiving Z-Wave certification after 2 April 2017. Developed in conjunction with cybersecurity hacking experts, S2 promises new levels of impenetrability by securing communications both locally for home-based devices and in the hub or gateway for cloud functions.

S2 removes the risk of devices getting hacked while included on the network, since devices are uniquely authenticated on the network via QR or pin-code included on the device itself. The addition of secure key exchange via Elliptic Curve Diffie-Hilman (ECDH) eliminates the threat of common hacks such as man in the middle and brute force, while the tunneling of Z-Wave over IP (Z/IP) traffic through a secure TLS 1.1 tunnel secures cloud communications.

Administering the standards of Z-Wave specifications, including S2 security solutions, are 3rd party test facilities in Europe, US and Asia.

Go Z-Wave Alliance Announces New Security Requirements for All Z-Wave Certified IoT Devices