Written by Marco Attard
12. 04. 2017

The Z-Wave Alliance announces all Z-Wave devices require "strict and uniform" adoption of the Security 2 (S2) framework, the most advanced security for connected devices, controllers, gateways and hubs available.



The alliance board unanimously voted in favour of the addition of the S2 framework back in November 2016. From April 2017 a technical certification program administered through 3rd party test facilities in Europe, US and Asia will check all new certified devices carry the correct implementation of S2 security solutions containing rules for command classes, timers and device types. S2 devices should also be backwards compatible with existing devices on the market.

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.

“We are absolutely committed to making Z-Wave the safest, most secure ecosystem of smart devices on the global market,” the Z-Wave Alliance says, “Our work, in conjunction with the entire Alliance membership, will ensure that developers, service providers, manufacturers and consumers alike will look to Z-Wave as the most trusted solution with the highest levels of protection.”

Go Mandatory Security Implementation for All Z-Wave Certified IoT Devices Takes Effect Today