DER Security and IEEE 2030.5

Robby Simpson, PhD
CTO, DER Security Corp.
Chair, IEEE P2030.5
VP, IEEE SA Board of Governors

December 2022
www.DERSec.io

Disclaimer

The following is my opinion and does not necessarily reflect that of IEEE, IEEE SA, IEEE P2030.5, etc.

DER Security Corp. Overview

- SunSpec Alliance sold all of its software assets to DERSec
- SunSpec is an OEM licensee of DERSec: reselling software under the SunSpec brand
  - SVP Dashboard
  - SVP DashBoard Plus Pack
  - Business as usual!
- Going forward, expanded focus on security and SaaS
- Welcome one-on-one discussions with interested parties!

IEEE 2030.5 Cybersecurity Highlights

- Utilizes TLS 1.2 with both client and server certificates
  - Designed to operate with little to no user intervention
- A number of national and international guidelines and requirements considered
- Geared toward embedded system constraints
- Mandatory Ciphersuite for interoperability: TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
- Optional PIN for authorization
- Firmware, software, and security update capability
- Many additional considerations, including:
  - Privacy
  - Grid security
- SunSpec operates a PKI / acts as a Certificate Authority

Why TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8?

- Based on NSA Suite B recommendations
- Geared toward embedded systems
- Same ciphersuite used by many other IoT standards and ecosystems
- CCM-8
  - Used in many IEEE 802 technologies (hardware reuse)

Why Allow/Denylists Instead of Revocation?

- Recommendation from IEEE 802.1AR
- Eliminates need for global, online revocation server
  - Difficult in multi-party, multi-vendor, standards ecosystems
  - Some IEEE 2030.5 devices may be isolated from wider Internet (and thus revocation server)
- Re-establishing trust in device difficult, to put it mildly

Thanks! Let’s talk!

Robby Simpson – robby.simpson@dersec.io