Zero-Trust Architecture and DNP

Why Zero-Trust

- Ensuring Continued Security of Critical Electric Infrastructure requires a new model of security: a Zero-Trust Architecture – based model for securing critical infrastructure and the supply chain

https://dnp.org/cstf

What is Zero Trust

- A “Zero Trust” model is a model in which **no asset or entity is trusted based on its physical or network location, or based on ownership**
- It requires **authentication of all sessions, assets, devices, users**, **authorization of all actions**, and **supply chain management** (e.g. electronic pedigrees, conformance certification, etc.)

How DNP addressed Zero Trust

- DNP3 Security Layer authenticates every message, session, and Controlling Station-Outstation Association providing mutual authentication
- The Authorization Management Protocol (AMP) provides the PKI to authenticate, authorization for Master-Outstation Associations, and the ingredients for RBAC
- AMP also provides means to implement an electronic pedigree using manufacturer-installed certificates
- RBAC is on the CSTF backlog
- Remote Attestation is envisioned as an extension to AMP (with device support), also on the CSTF backlog
- DNP-UG already has a certification program, and certification procedures for DNP3 and DNP3 SAv5

What’s Next

- Currently drafting a document to outline how DNP addresses Zero Trust
- Continuing the development work on DNP3-SAv6 and AMP

For further information please contact: chair_tech@dnp.org or admin@dnp.org