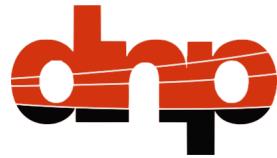


# The DNP Security Session Layer (DNP3-SL)



Developed by the **DNP Cybersecurity Task Force (CSTF)** in collaboration with **IEC Technical Committee 57 Working Group 15**, DNP3-SL is the **DNP3 Security Layer (formerly Secure Authentication Version 6 - SAv6)..**

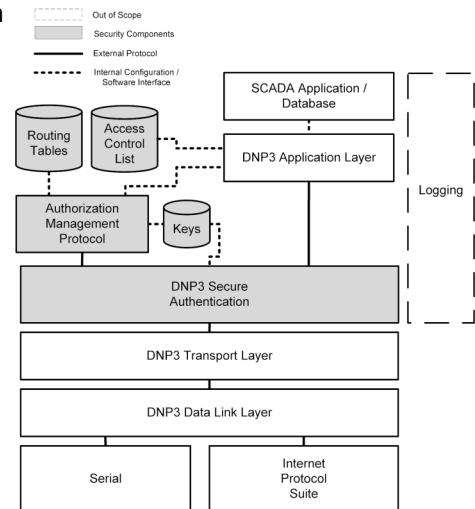
DNP3-SL is an implementation of the new **IEC 62351-5 International Standard**



<https://dnp.org/cstf>

## Features

- Provides **authentication and integrity** between devices at the application layer
- **Supports message encryption**
- **Will use post-quantum cryptography** for Association establishment
- Uses Hash-Based Message Authentication Codes (HMACs) and/or Authenticated Encryption with Additional Data (AEAD)
- Defined as separate layer that **can be used for other protocols**
- **Simplified procedures** and new algorithms in this version
- Authenticates all messages and eliminates previous inefficient challenge-response
- Can co-exist with DNP3-SAv5

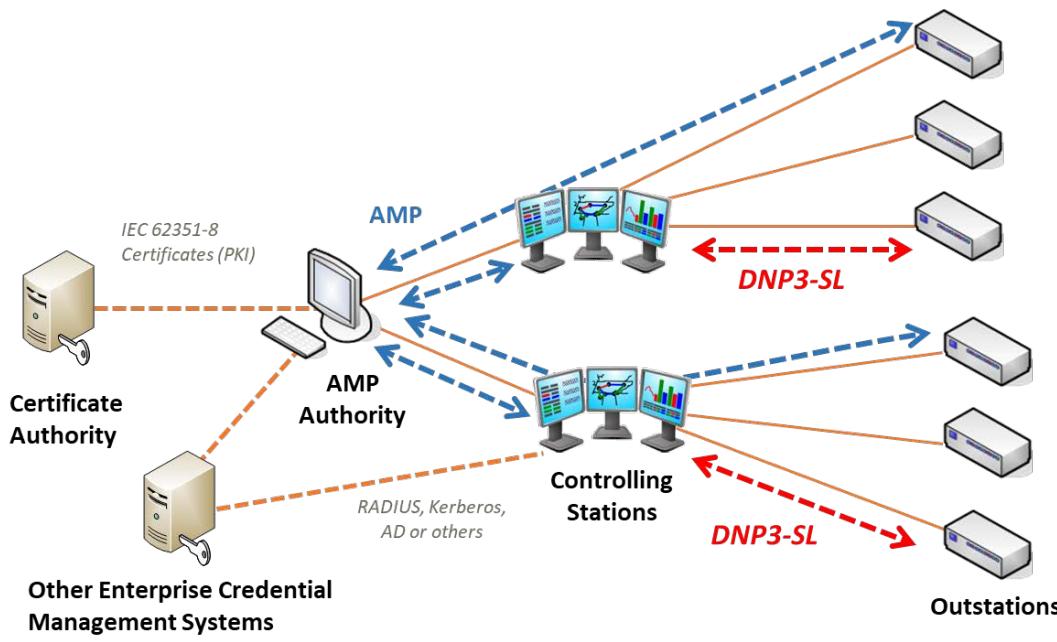


## Design principles

- Simple to implement using modern tools.
- No unnecessary complexity.
- Use known, proven, and widely-implemented primitives as much as possible
- Use standard methods, formats, algorithms, and concepts as much as possible, e.g. X.509 certificates, ML-KEM key establishment
- Does not use pre-set keys, i.e. no human access to any shared secrets

## Integration with Public Key Infrastructure (PKI)

- Integrates with the Authorization Management Protocol (AMP) or other PKI



# The Authorization Management Protocol (AMP)



Developed by the **DNP Cybersecurity Task Force (CSTF)**, the Authorization Management Protocol **Authenticates** devices that implement AMP, **Authorizes** communications between DNP3 Application Layers, and **Manages** security policies.



<https://dnp.org/amp>

## Features

- Centralized authorization and management of **IP-based, serial, and hierarchical networks**
- Implements an **IEC 62351-5 Central Authority**
- **Role-Based Access Control (RBAC)** including systems with multiple areas of responsibility
- Security managers can promptly revoke authorization and/or privileges to quickly regain control after an attack
- Allows devices to generate their own keys, avoiding personnel viewing security secrets
- **Accommodates redundant connections, Controlling Stations, and Authorities**
- Transports defined for AMQP and DNP3-SL
- **Can be used separately** with protocols other than DNP3

## Authentication

- **Uses X.509 Identity Certificates** for the Authority and devices to authenticate each other
- The Authority can be part of a full **Public Key Infrastructure (PKI)** including an Intermediate Certificate Authority associated with the Authority itself, or can provide the PKI as needed.
- All managed devices have an Authority-signed certificate.
- All AMP messages are digitally signed and most are encrypted

## Authorization

- **Uses X.509 Attribute Certificates** to convey RBAC info as well as access authorization
- Implements industry-standard **IEC 62351-8 RBAC** definitions
- Can use a single attribute certificate to authorize one or many **Controlling Station-Outstation Associations**

## Security policy management

- Permits network managers to set and distribute critical **policies for system-wide security management**, e.g. tell each device through the protocol itself:
  - How to identify the Authority
  - How often to update credentials
  - How to behave when the Authority is not available
- **Protects against replay and spoofing of policies**, and keeps policies confidential

*Policies enable system availability and continued operation*

