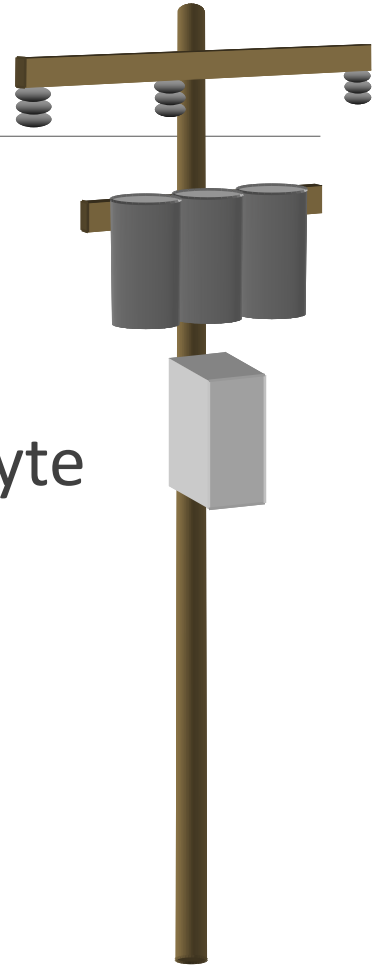
#DISTRIBUTECH24 // DISTRIBUTECH.COM

How DNP3-SAv6 and AMP Meet OT Security Requirements Like Nothing Else

Grant Gilchrist, P. Eng
Tesco Automation
DNP Users Group

DISTRIBUTECH INTERNATIONAL
EDUCATION: FEBRUARY 26-29, 2024
EXHIBITION: FEBRUARY 27-29, 2024
Orange County Convention Center
Orlando, Florida, USA

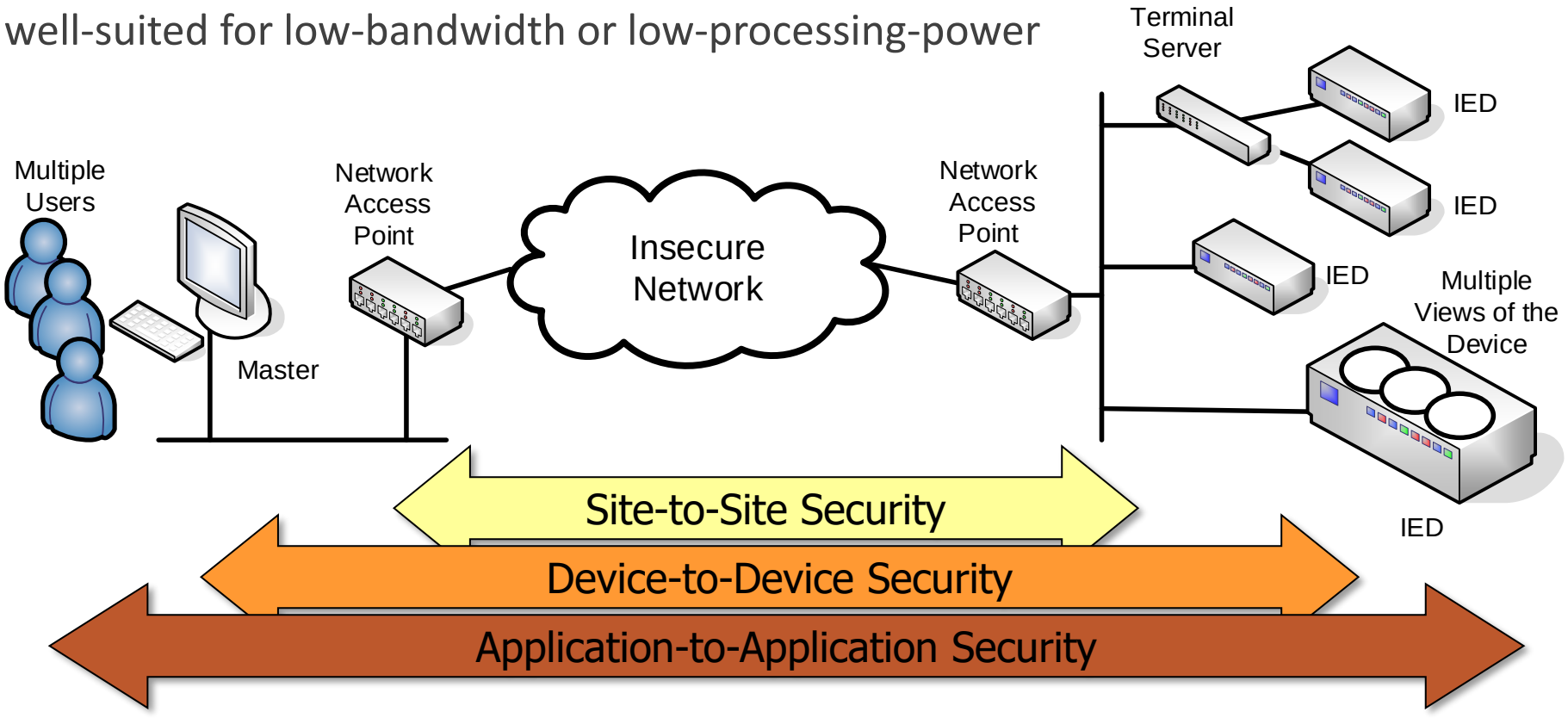
The SCADA Environment



- Very challenging for implementing security
- Mixed IP-based and serial networks
- Serial is low-bandwidth, unreliable, sometimes pay-per-byte
- Devices typically have low processing power
- Use data concentrators, not routers
- Security server access available only at topmost nodes

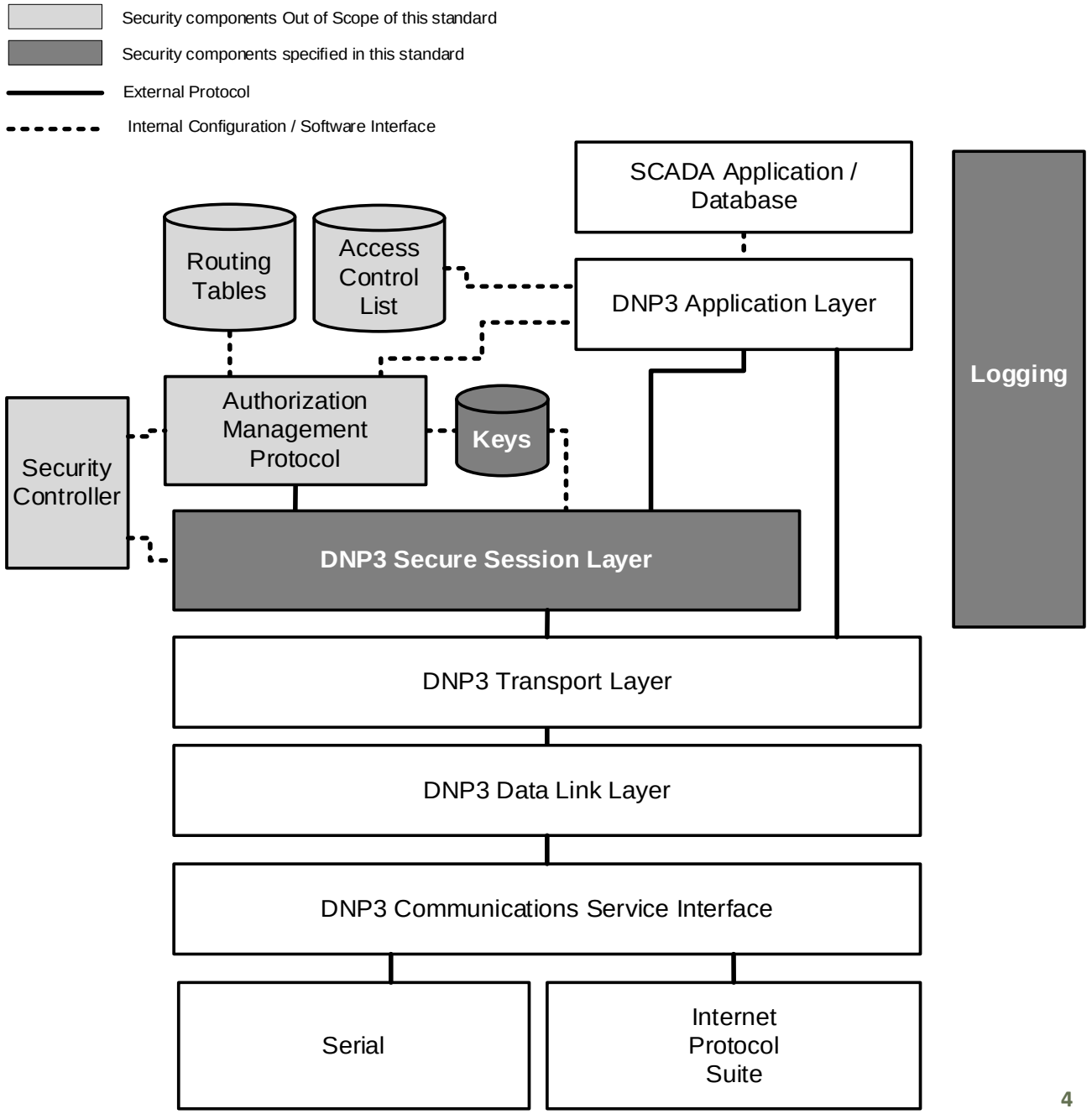
Why Not Use TLS or IPSec?

- They only reach to the borders of the IP network
- Do not reach serial devices
- Not well-suited for low-bandwidth or low-processing-power

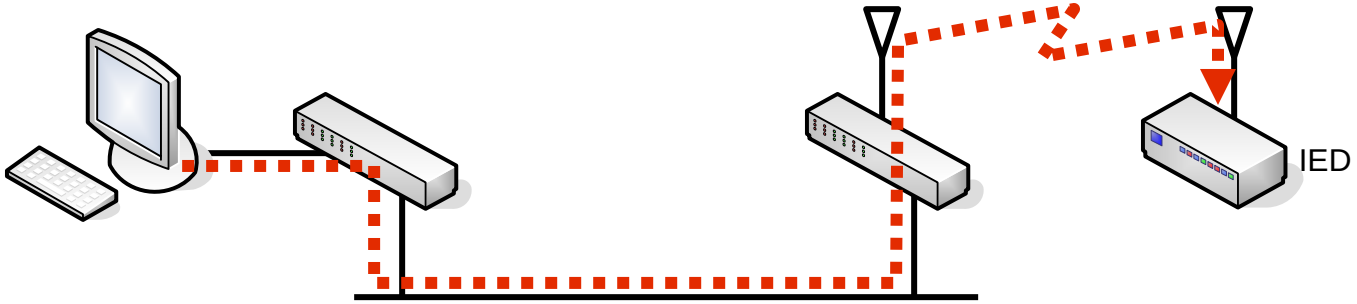


Solution: The DNP3 Security Architecture

- To be published in IEEE Std 1815

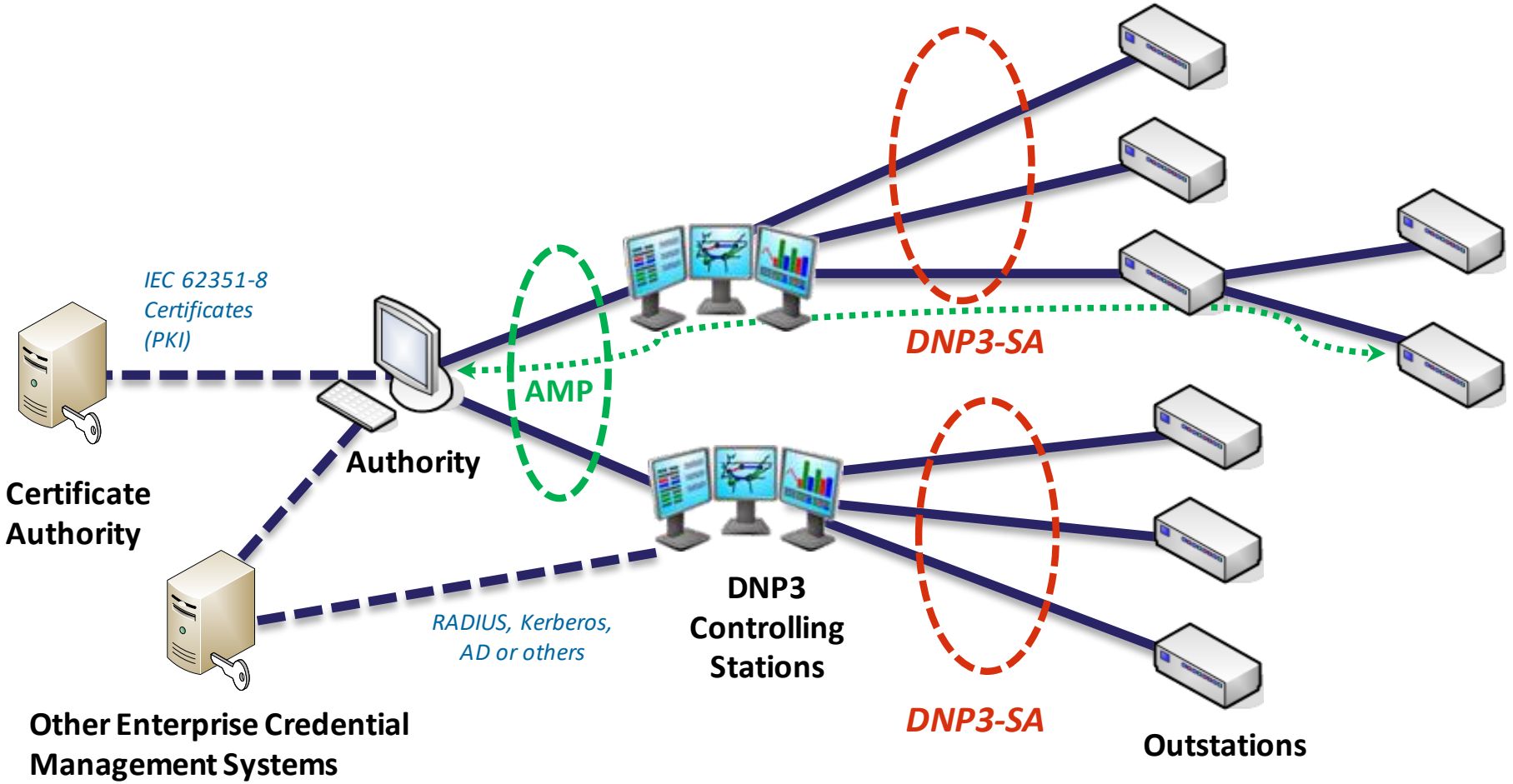


Secure Over Serial, TCP/IP or Radio



- Security carried at session layer, just below DNP3
- Helps utilities concerned about “routable protocols”
- Works with terminal servers and IP Radios

Integration with the Enterprise



Benefits and Features

DNP3-SAv6

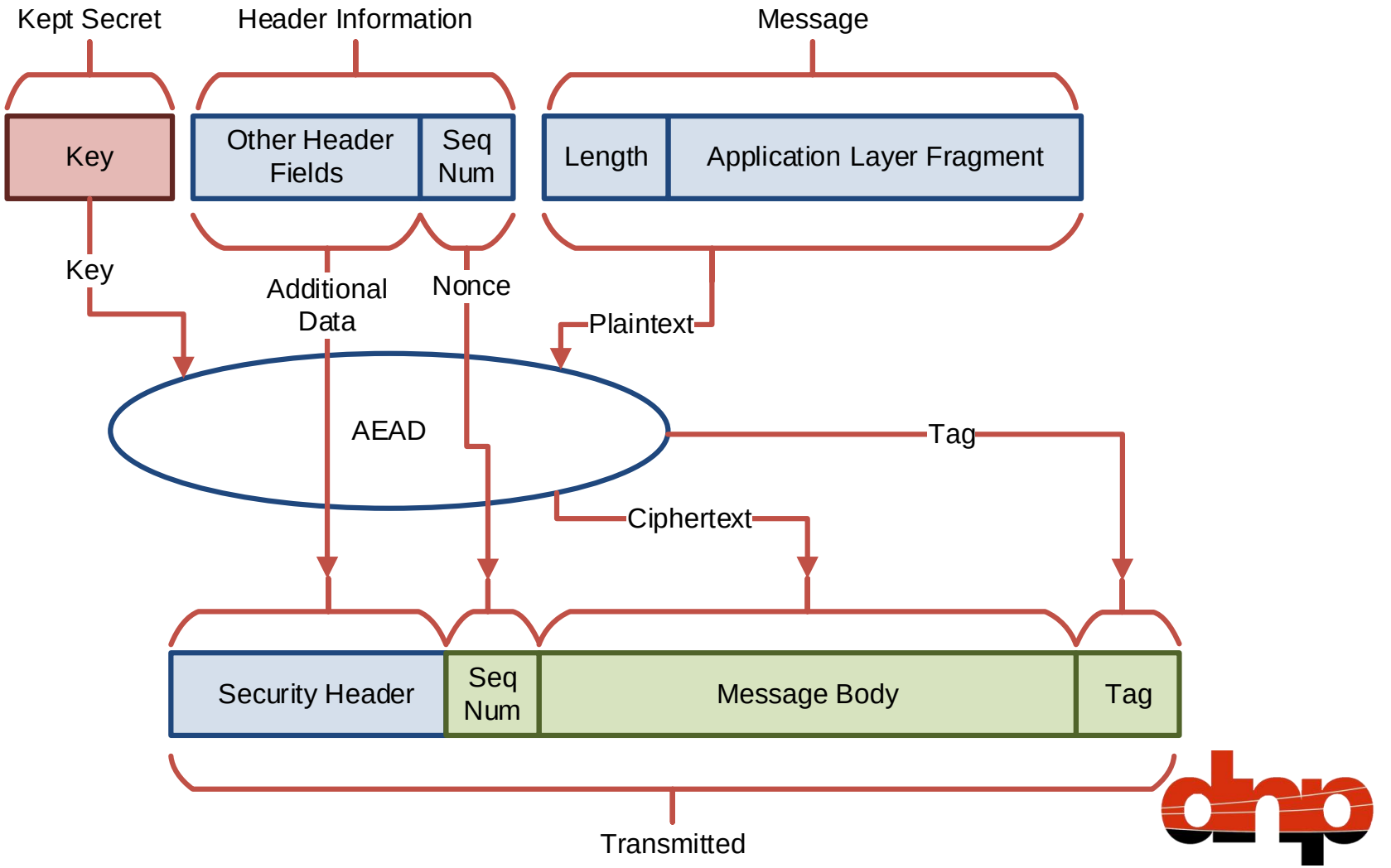
- Authentication, integrity and RBAC between devices at ***application layer***
- Uses Hashed Message Authentication Code (HMAC)
- Now also supports ***encryption***
- Defined as ***separate layer*** that can be used for other protocols
- ***Elliptic curve*** algorithms to minimize processing power
- Simplified procedures and new algorithms in this version
- Can be used with AMP or other PKI

AMP

- Central authorization for ***both IP and hierarchical serial*** networks
- Promptly revokes authorization and/or privileges through RBAC
- Allows devices to generate their own keys, ***avoiding human interaction***
- Accommodates redundant connections, masters and authorities
- Prevents tunneling of non-DNP3 messages
- Can be used ***separately*** with other protocols

Authentication and Encryption of Messages

- Key is never transmitted
- Tag is created by scrambling and truncating the message
- The tag sent with the message must match that calculated with local copy of the key
- Nonce prevents replay attacks
- Called a MAC if not encrypted

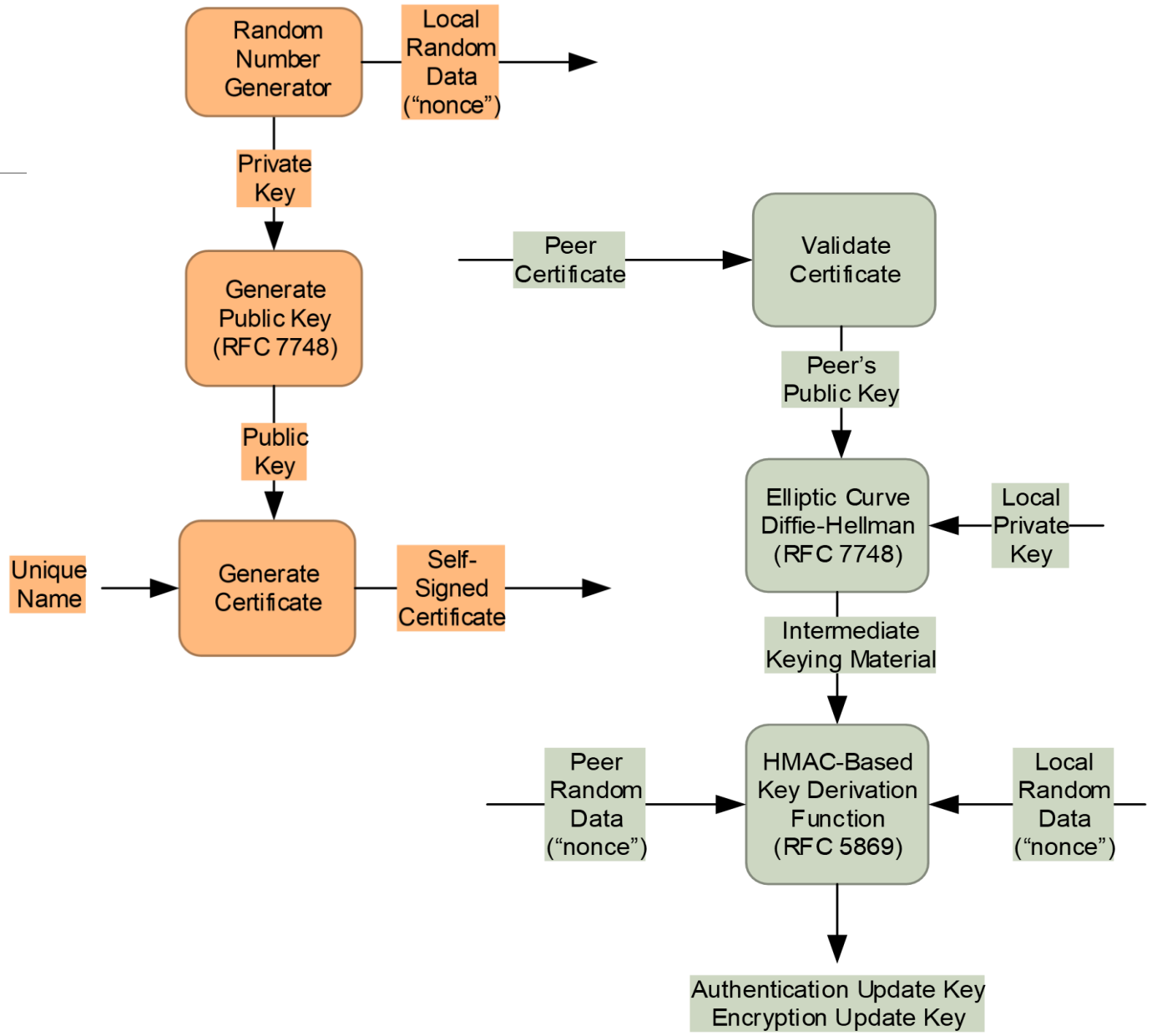


Three Layers of Keys

Type	How Many?	Used to…	Change how often?
Session Keys	Monitoring Direction Key Control Direction Key	Authenticate and optionally encrypt DNP3/IEC 60870-5 messages	Minutes up to weeks
Update Keys	Encryption Key Authentication Key	Encrypt new Session Keys; authenticate the association and session setup sequences	Months or years
Asymmetric Keys	Private Key Public Key	Sign certificates, establish an association, and independently generate Update Keys from the Public Keys and random data	Determined by utility policy; usually years

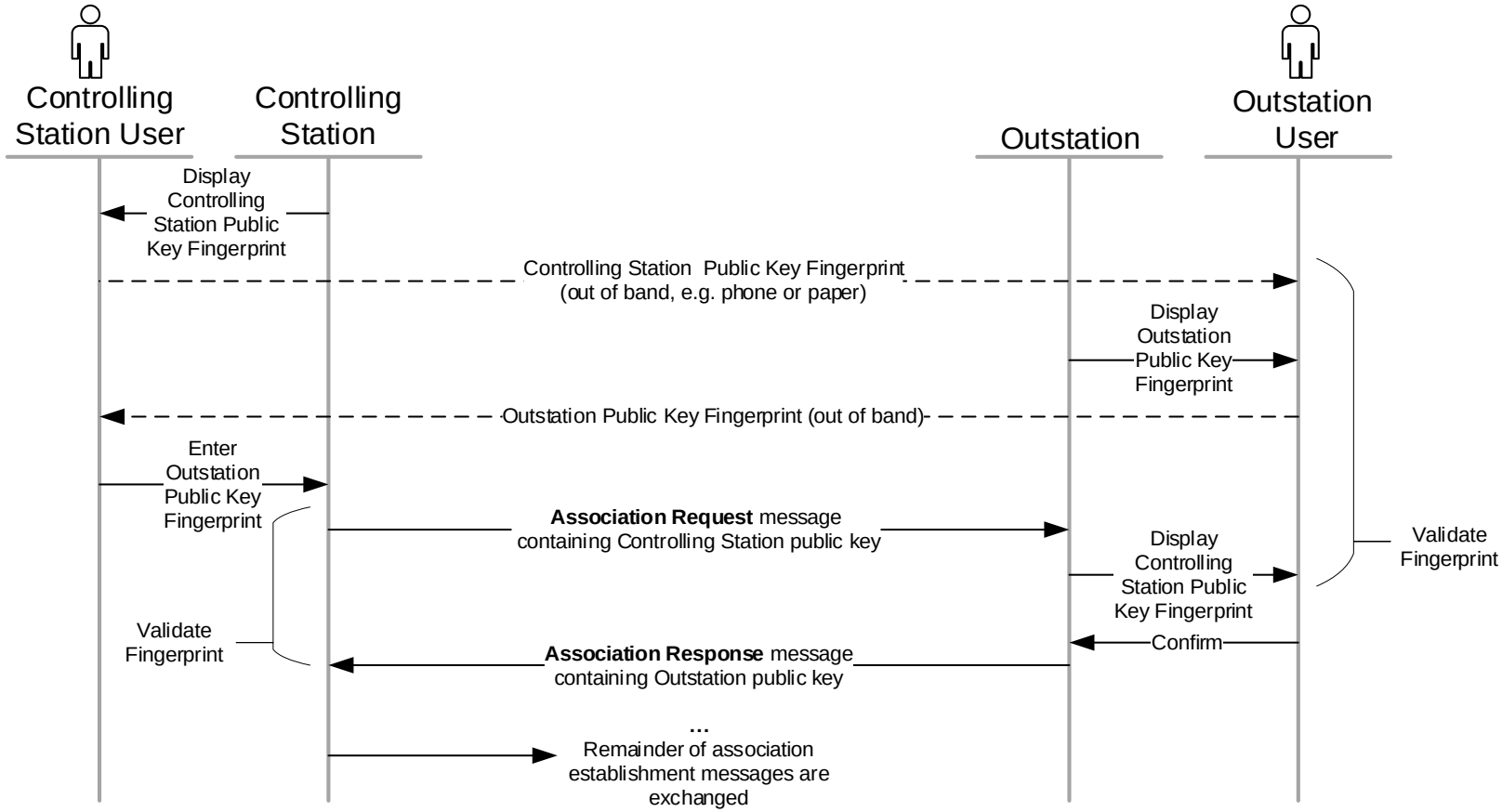
Association Establishment

- Master and Outstation exchange random data and certificates
- Both independently generate a common symmetric “Update Key” for encrypting DNP3-SAv6 Session Keys
- Uses Elliptic Curve Diffie-Hellman (ECDH) and HMAC-based Key Derivation (HKDF) algorithms
- MACs are generated as part of the same process that creates the Update Keys



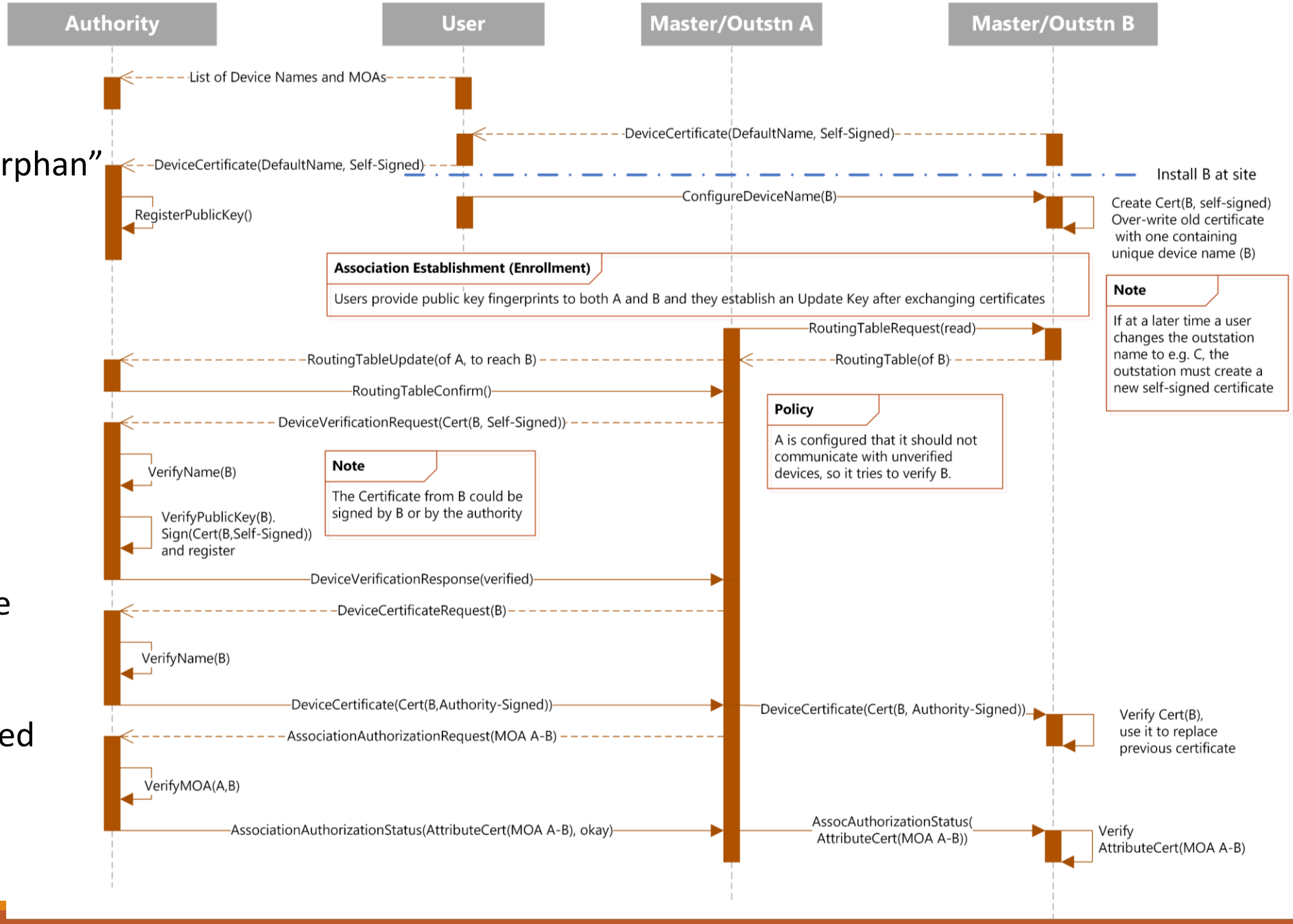
Field Device Enrollment

- Certificates of controlling station and outstation may be **self-signed**
- Permits installation and authorization of devices **without connection to an Authority**
- Humans exchange **public key fingerprints** (BIP-39 mnemonic word code)
- They **do not need to handle** certificates or keys
- No need for complex user interface at outstation

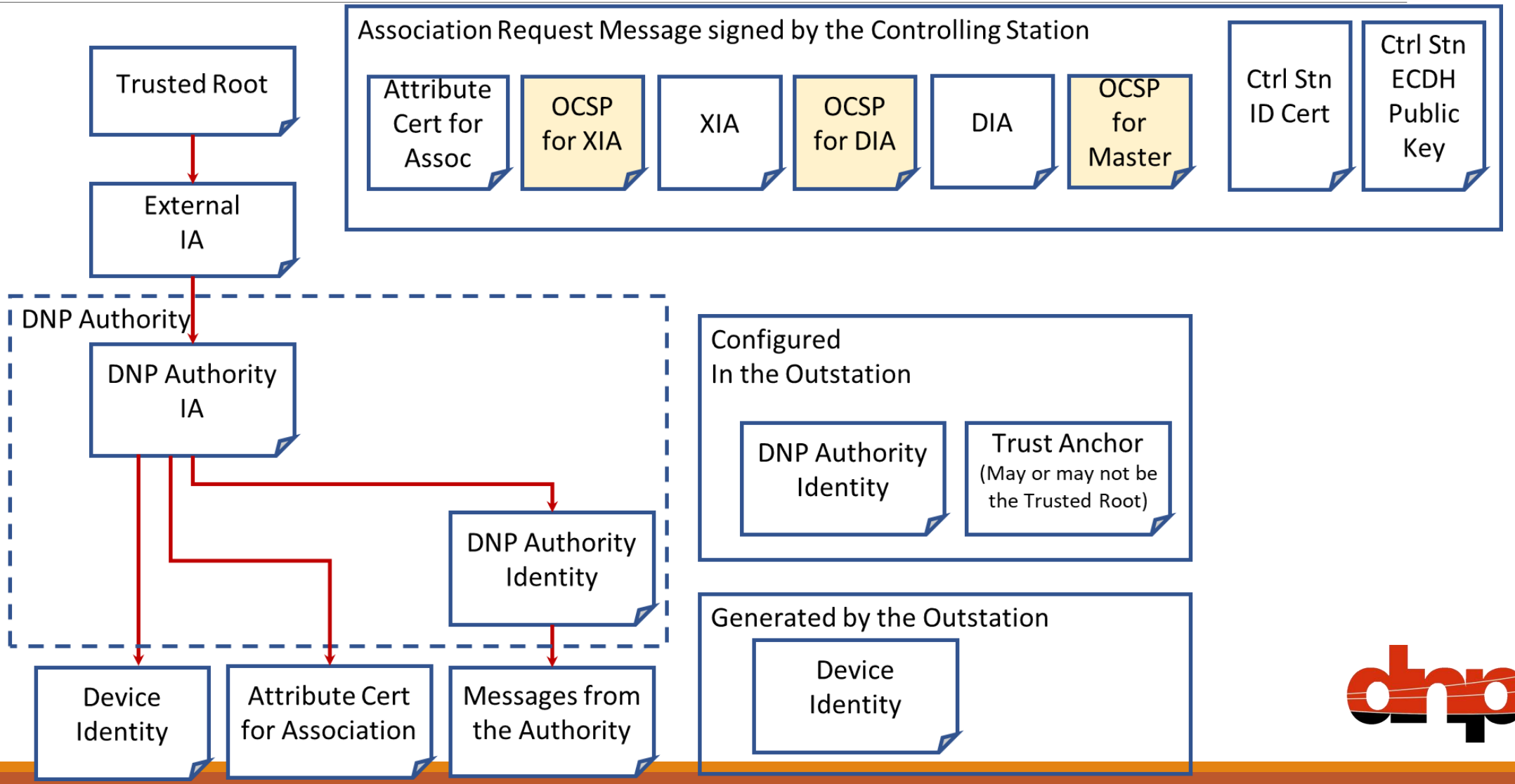


AMP Example

1. Outstation registers as “orphan”
2. Outstation configured
3. Association established
4. Routing table updated
5. New outstation verified
6. New outstation certificate
7. New association authorized
8. New master certificate



AMP Certificates and Authorities

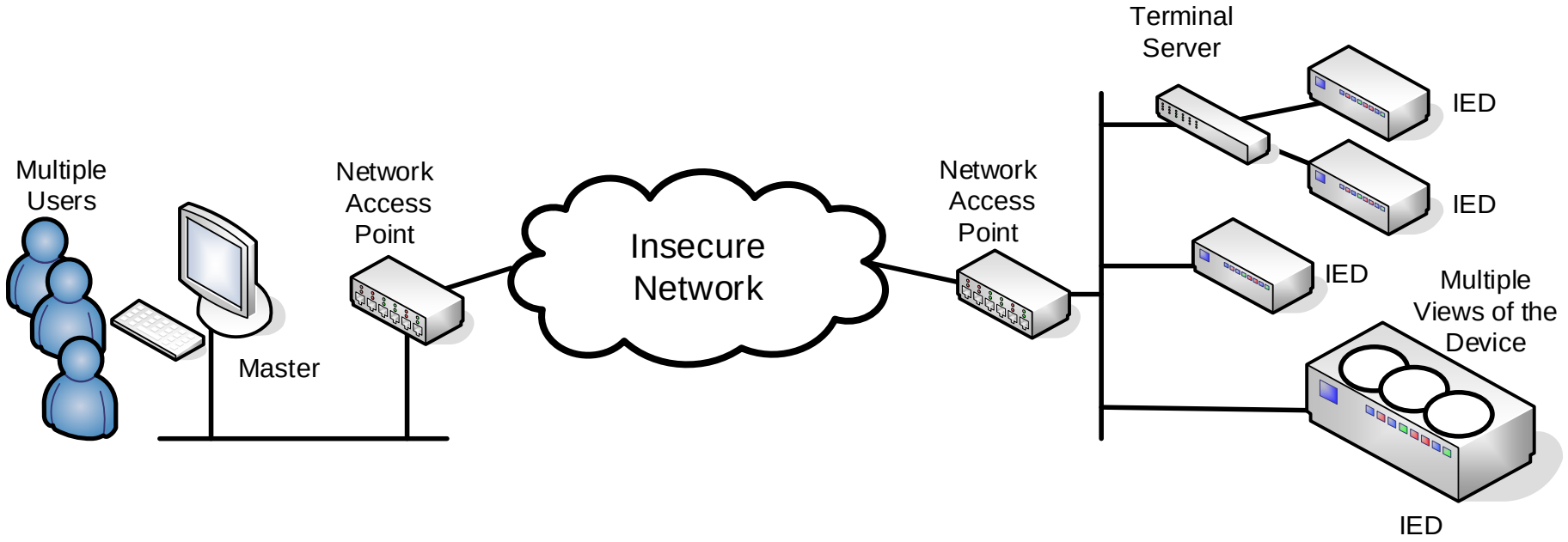


Status of the Standards

- DNP3-SAv6
  - Included in the current draft IEEE Std 1815
  - Reviewed by DNP Users Group Cyber-Security Task Force and IEEE P2 Working Group
  - Will be submitted for ballot shortly
- AMP
  - Will become its own document
  - Initially released by DNP Users Group, then standardized
  - Message formats and use cases identified
  - Development of an AMP Authority underway – will be productized
  - Specification of procedural behaviors in progress

Summary: AMP and DNP3-SAv6

- They not operate just over IP but also over mixed serial and IP networks
- They permit enrollment without humans seeing any security keys
- They permit management of devices that existing IT tools can't reach
- The secure session layer (DNP3-SAv6) will be part of IEEE Std 1815 shortly



#DISTRIBUTECH24 // DISTRIBUTECH.COM

TESCO

dnp

DISTRIBUTECH® INTERNATIONAL

ORGANIZED BY: CLARION ENERGY

OFFICIAL MEDIA BRAND: POWER GRID INTERNATIONAL

HOST UTILITY: DUKE ENERGY.

Grant Gilchrist, P. Eng.
Systems Engineer, Grid Modernization
+1-403-991-5343
ggilchrist@tescoautomation.com
grant.gilchrist@ieee.org

EDUCATION: FEBRUARY 26-29, 2024
EXHIBITION: FEBRUARY 27-29, 2024

Orange County Convention Center
Orlando, Florida, USA