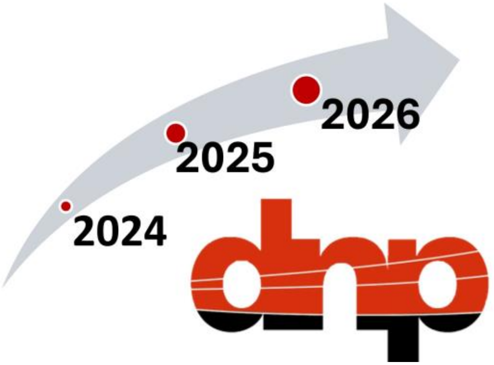
# VISION 2024 - Background

May 2024

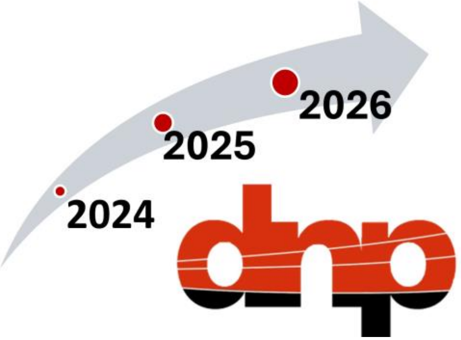
Board of Directors, DNP Users Group



# Outline

- Overview and Mission of the DNP-UG
- Industry Trends
- Rationale for membership
- Update on 2023 programs and activities
- Strategic and tactical plans for 2024

DNP Users Group = DNP-UG



# Overview of the UG

- The UG actively manages DNP3:
  - **New** standard IEEE 1815.2™ (DER communications) due 2025
  - **Next** edition of IEEE 1815™ (includes SAv6) due 2025
  - **New** Authorization Management Protocol (AMP) development continues
  - Promotion and standards involvements
  - Technical Committee develops enhancements and corrections in the form Technical Bulletins
  - Technical Bulletins and other updates are merged into revisions of IEEE 1815™
  - Application Notes published to address specific applications
  - Guides provide additional information and help
- Four technical teams:
  - Technical Committee
  - Cybersecurity Task Force
  - Test Management Committee
  - Test Procedure Committee
- Board of Directors
- Funding sources:
  - Membership fees (primary)
  - Partnership Program

Image by storyset on Freepik

# DNP Users Group Mission Statement

- We actively develop and support measures to improve interoperability and cybersecurity in DNP systems by developing technologies and standards, implementing a conformance program, and providing education to the industry.
- Our over-arching goals:
  - Reduce utility project cost and risk.
  - Reduce vendor development cost and risk

# Mission of the DNP-UG

**To Actively Develop and Support Improved:**

1. **Interoperability**
   - Test procedures
   - Conformance certification
   - Device profile (XML and Word formats)
   - Application specific profile (DER)
   - Technical bulletins and standard updates
   - Application notes
   - Guides
2. **Cybersecurity**
   - Secure Authentication Version 5 (SAv5)
   - Secure Authentication Version 6 (SAv6)
   - Authorization Management Protocol (AMP)
   - Technical bulletins and standard updates
   - Application notes
   - Guides
3. **Education**
   - New workshops and tutorials
   - User forum (website)
   - Expert assistance (per membership level)
   - Technical bulletins
   - Application notes
   - Guides

**Key Focus Area - DER Communications**

- IEEE 1815.2 – DNP3 Profile for DER Communications
- Conformance certification
- MOU with MESA

# Industry Trends

- **Pressing need for defense in depth – OT Cybersecurity**
  - The DNP-UG's next generation cybersecurity specifications are uniquely applicable to the critical OT communications link usually using DNP3
- **Interoperability is an ongoing challenge for the industry**
- **DER communications and cybersecurity is a growing imperative**
- **From devices/system to holistic solutions**
  - Holistic solutions from multiple vendors integrate well
  - Must be standards based
  - Strive to maximize interoperability, including conformance certification
  - Important to reduce the number of standards

# Update on 2023 Programs and Activities (1)

**Interoperability:**

- Test procedures (new)
- Device profile guidance
- Update to IEEE Std 1815™
- Conformance Certification Program

**Cybersecurity:**

- Secure Authentication Version 5 (SAv5) – currently available.
- Secure Authentication Version 6 (SAv6) & Authorization Management Protocol (AMP) –

continued development.

- Roadmap to support Zero Trust over serial and IP.
- DOE proposal

# Update on 2023 Programs and Activities (2)

**DER Communications:**

- MOU with MESA
- Significant contributions to new standard IEEE P1815.2 (DER Communications). Chair and co-editor
- Support MESA on the MESA-DER DNP3 Profile Test and Certification Program
- Normative references to DNP3 in IEEE Std 1547-2018$^{\text{TM}}$
- Normative references SAv5 and SAv6 in IEEE 1547.3$^{\text{TM}}$

**Over 4,000 hours of volunteer effort** by industry leaders and top talent across our five operating committees and task forces.

**New PT staff for membership engagement**

# Strategic and Tactical plans for 2024

- **Tactical Plans:**
  - New fee structure for 2024
  - Courses at DistribuTECH
  - Changes to TC Charter
  - Changes to Conformance Certification Program
    - Planning for DER vendor group
    - Engage with UL in support of MESA T&C
    - Formalize offering for SAv5

- **Strategic Plans:**
  - Continuing development of AMP
  - Start test procedure development for SAv6
  - Strong effort on 1815.2 to ballot
  - Big push on 1815 to ballot (includes SAv6)
  - Participation if funding permits – CISA CSWG and IEEE 1547.10.
  - Expand service offerings e.g., training, consulting
  - Grow engagement with utilities and other members
  - Expand role of membership engagement staff
  - Website improvements

# Rationale for Membership (1)

- **Engineering level benefits:**
  - Continued availability to our standards including updates.
  - Awareness of helps the UG provides such as the Device Profile Guide.
  - Access to other related documentation such as test procedures and tutorial information.
  - On-going enhancements with new features and updates.
  - List of Conformance Certified Products
  - The opportunity to participate in one or more of our operating committees to learn and contribute.
  - **Access to training, forum, workshops and lessons learned (future).**

# Rationale for Membership (2)

- **Strategic level benefits:**
  - A holistic system approach, when using multiple vendor's products, assumes a higher degree of interoperability, reliability and security of communications provided by DNP3.
  - Lower product development (vendors) and project deployment costs and risks (utilities) are the result of the work of the DNP-UG (e.g., test procedures, guides, Conformance Certification Program).
  - Utilities gain from using the latest technology with the most functionality providing the greatest economic and operational benefits.
  - Other utilities are participating in the UG and implementing and benefiting from the most current functionality.
  - DNP3 is widely used (~94% of utilities) which provides economies of scale with the lowest possible costs to all users.
  - Industry visibility and reputational benefits a partner of the DNP-UG.

# Rationale for Membership (3)

- **Summary:**
  - Broad input by experts and thought leaders improves our developments!
  - Without the DNP-UG supporting DNP3, successful interoperability among different vendor's devices would be much more expensive or not possible at all.
  - Strong support of the DNP-UG will enable thousands of volunteer hours (over 4,000 hours in 2023) per year by industry experts in key programs driving improved cybersecurity and interoperability.
  - A viable DNP-UG will continue to execute on our mission of maximizing interoperability, improving cyber security, optimizing DER communications.

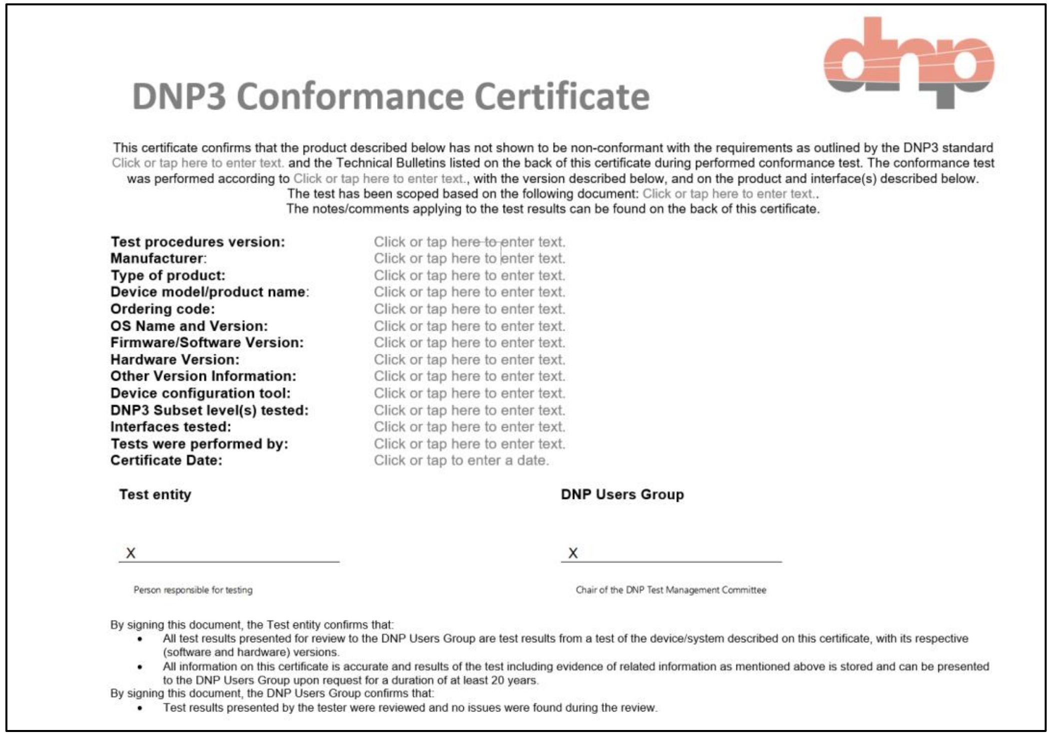
# Next Steps

- Follow the DNP Users Group on LinkedIn for more updates.
- Reach out to Sara at admin@dnp.org for more information and assistance with memberships.
- Please join the UG today!

# Back-up Material

# Conformance Test Review (CTR) Process

- Improved assurance of interoperability including SAv5
- Reduced program risk
- Recommended for all new or updated products
- Expert review of Device Profile and Test Logs



## DNP3 Conformance Certificate

This certificate confirms that the product described below has not shown to be non-conformant with the requirements as outlined by the DNP3 standard Click or tap here to enter text. and the Technical Bulletins listed on the back of this certificate during performed conformance test. The conformance test was performed according to Click or tap here to enter text., with the version described below, and on the product and interface(s) described below.
The test has been scoped based on the following document: Click or tap here to enter text..
The notes/comments applying to the test results can be found on the back of this certificate.

| | |
|---|---|
| **Test procedures version:** | Click or tap here to enter text. |
| **Manufacturer**: | Click or tap here to enter text. |
| **Type of product:** | Click or tap here to enter text. |
| **Device model/product name**: | Click or tap here to enter text. |
| **Ordering code:** | Click or tap here to enter text. |
| **OS Name and Version:** | Click or tap here to enter text. |
| **Firmware/Software Version:** | Click or tap here to enter text. |
| **Hardware Version:** | Click or tap here to enter text. |
| **Other Version Information:** | Click or tap here to enter text. |
| **Device configuration tool:** | Click or tap here to enter text. |
| **DNP3 Subset level(s) tested:** | Click or tap here to enter text. |
| **Interfaces tested:** | Click or tap here to enter text. |
| **Tests were performed by:** | Click or tap here to enter text. |
| **Certificate Date:** | Click or tap to enter a date. |

| **Test entity** | **DNP Users Group** |
|---|---|
| X ____________________ | X ____________________ |
| Person responsible for testing | Chair of the DNP Test Management Committee |

By signing this document, the Test entity confirms that:

- All test results presented for review to the DNP Users Group are test results from a test of the device/system described on this certificate, with its respective (software and hardware) versions.
- All information on this certificate is accurate and results of the test including evidence of related information as mentioned above is stored and can be presented to the DNP Users Group upon request for a duration of at least 20 years.

By signing this document, the DNP Users Group confirms that:

- Test results presented by the tester were reviewed and no issues were found during the review.

# Conformance Certification Program – Getting Started

- DNP-UG employs a CTR coordinator to handle the day-to-day management of the CTR process, as overseen by the TMC
- DNP-UG strongly recommends that devices are certified periodically to ensure compliance
- Two phases in the CTR Process:
  - Device Profile review
  - Test Logs review
- Get started by contacting: conformancetesting@dnp.org or contact:
  - Deryk Yuill at deryky@ieee.org
  - Ron Farquharson at r.farquharson@ieee.org

# DNP-UG Protocol Conformance Issue Tracking Summary

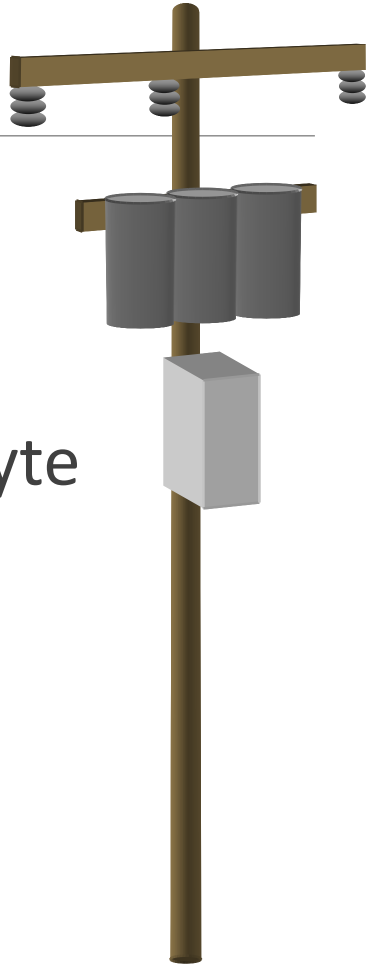
| No. | Device Type | Issue Found | Impact |
|---|---|---|---|
| 1 | Outstation | No class support | Master is not able to read data from outstation |
| 2 | Outstation | Partial Event Class Polling | Outstation fails when polled by master |
| 3 | Outstation | Data Link Reset is incorrectly required | Outstation will not communicate with some masters |
| 4 | Outstation | Broadcast not supported | Outstation will not participate in a system-wide freeze commands and might not permit correct time setting via DNP3 |
| 5 | Outstation | No support for UDP | Some expected functions will not work |
| 6 | Outstation | SBO command process not implemented correctly | A command may be operated in response to receiving an invalid or corrupted message |
| 7 | Outstation | Incorrect unsolicited configuration | Depending on network topology, configuration of timeouts, etc., all communications between the master and outstations stopped |
| 8 | Outstation | When replying to an integrity poll, static data is sent before event data | Operators could be shown incorrect data on their displays, which could lead to wrong actions. |
| 9 | Controlling Station | Unable to issue valid integrity poll | Operators could be shown incorrect data on their displays, which could lead to wrong actions. |
| 10 | Controlling Station | Reads frozen counter, never issues counter freeze | Unable to read frozen counter data from some devices |

# DNP-UG Cybersecurity Program

Summary as of April 2024

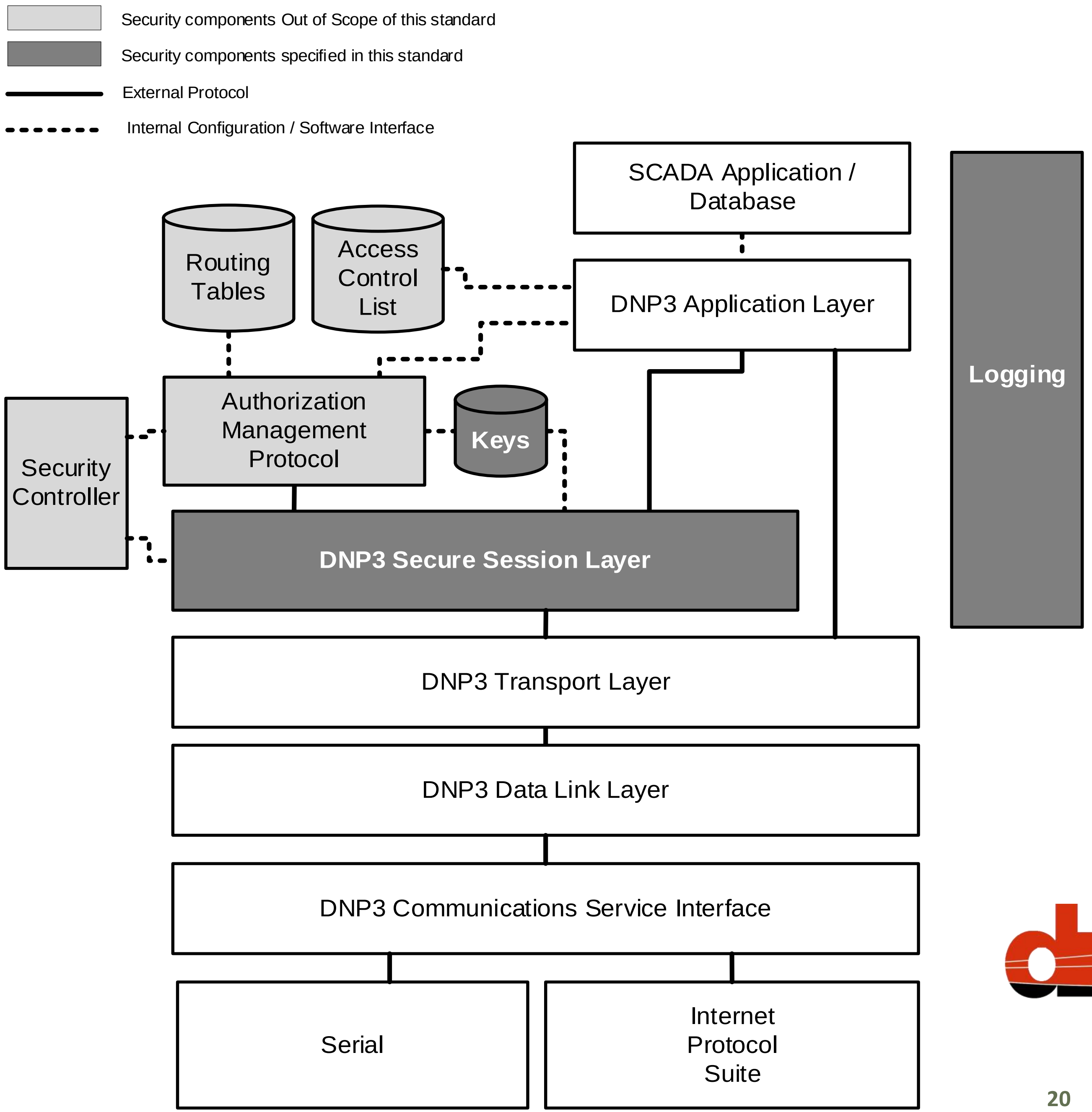
# The SCADA Environment

- 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

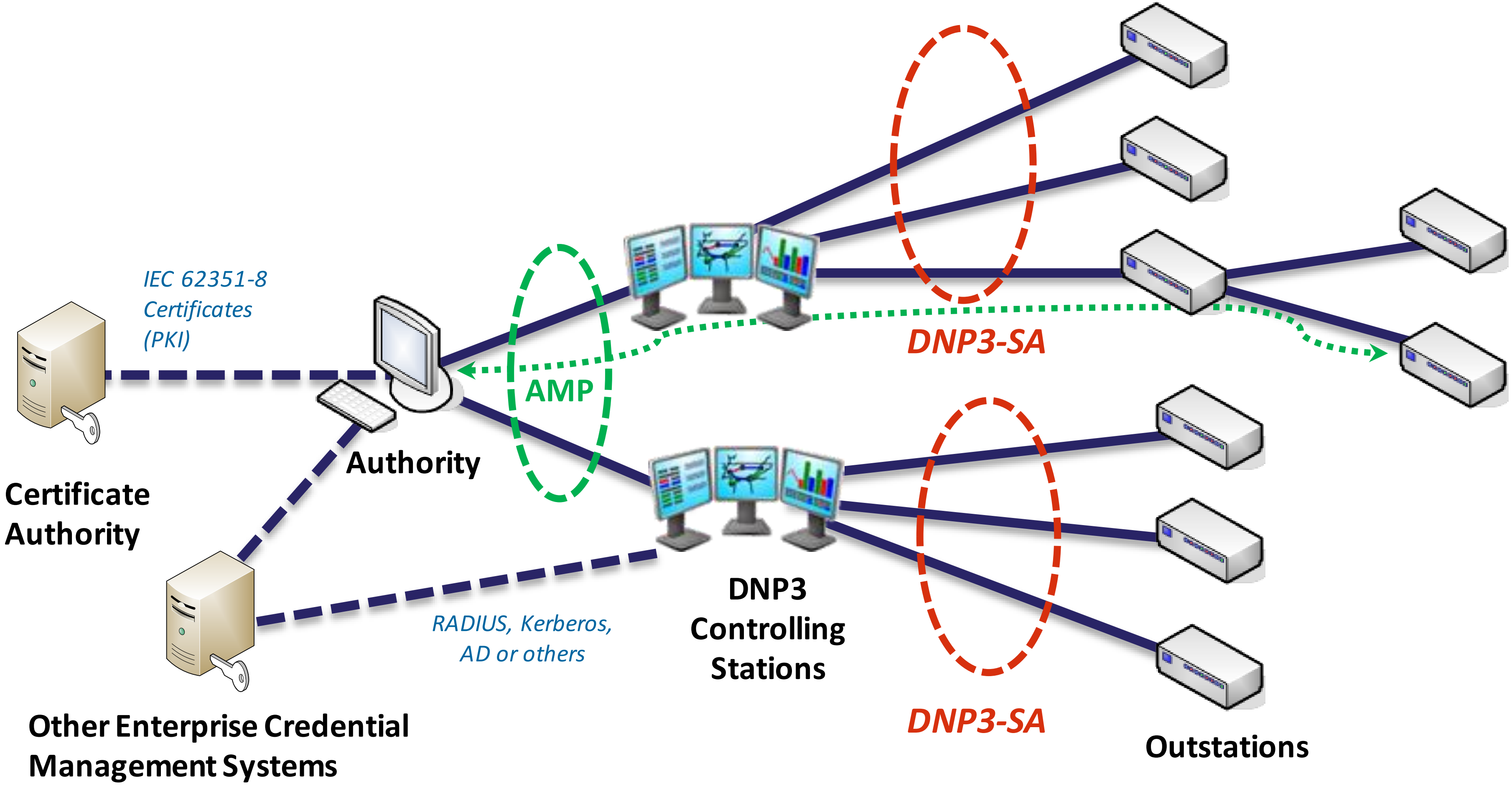


# Solution: The DNP3 Security Architecture

- To be published in IEEE Std 1815


Security components Out of Scope of this standard
Security components specified in this standard
External Protocol
Internal Configuration / Software Interface
SCADA Application / Database
Routing Tables
Access Control List
DNP3 Application Layer
Logging
Authorization Management Protocol
Keys
Security Controller
DNP3 Secure Session Layer
DNP3 Transport Layer
DNP3 Data Link Layer
DNP3 Communications Service Interface
Serial
Internet Protocol Suite

# Integration with the Enterprise



# Benefits and Features

## Secure Authentication v6 (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

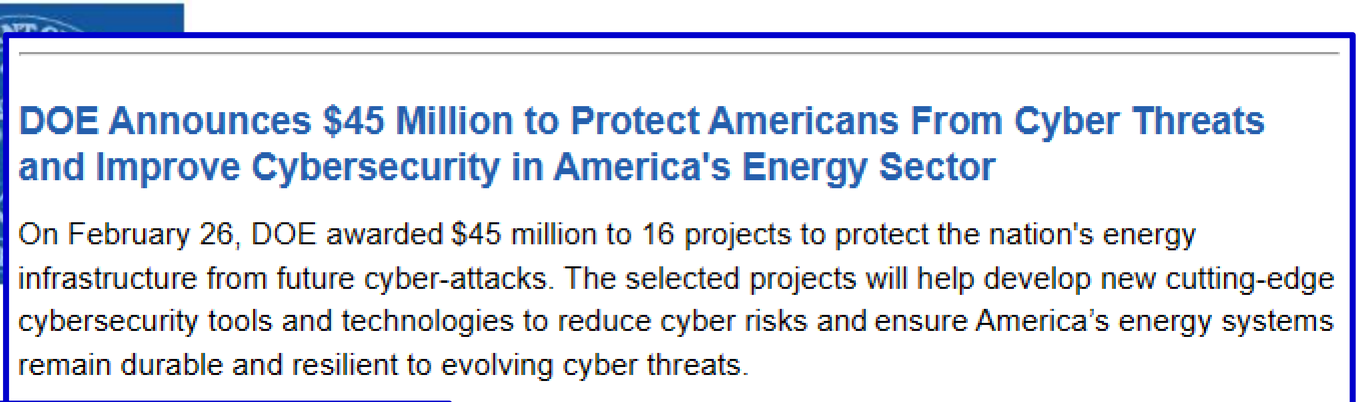
## Authorization Management Protocol (AMP)

- 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

# DOE Announcement – FOA 2500

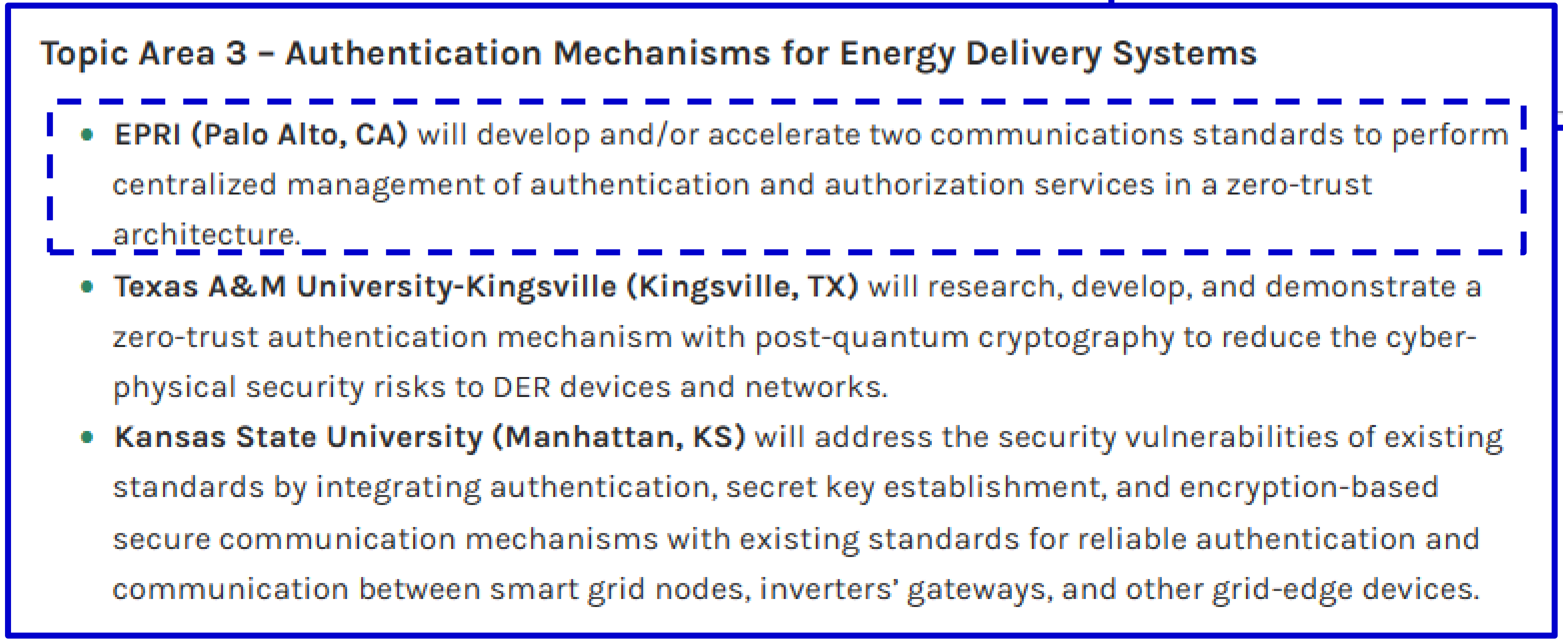
CESER
News & Updates
U.S. DEPARTMENT OF ENERGY
Office of Cybersecurity, Energy Security, and Emergency Response

The Latest From CESER



**DOE Announces $45 Million to Protect Americans From Cyber Threats and Improve Cybersecurity in America's Energy Sector**

On February 26, DOE awarded $45 million to 16 projects to protect the nation's energy infrastructure from future cyber-attacks. The selected projects will help develop new cutting-edge cybersecurity tools and technologies to reduce cyber risks and ensure America's energy systems remain durable and resilient to evolving cyber threats.



**Topic Area 3 – Authentication Mechanisms for Energy Delivery Systems**

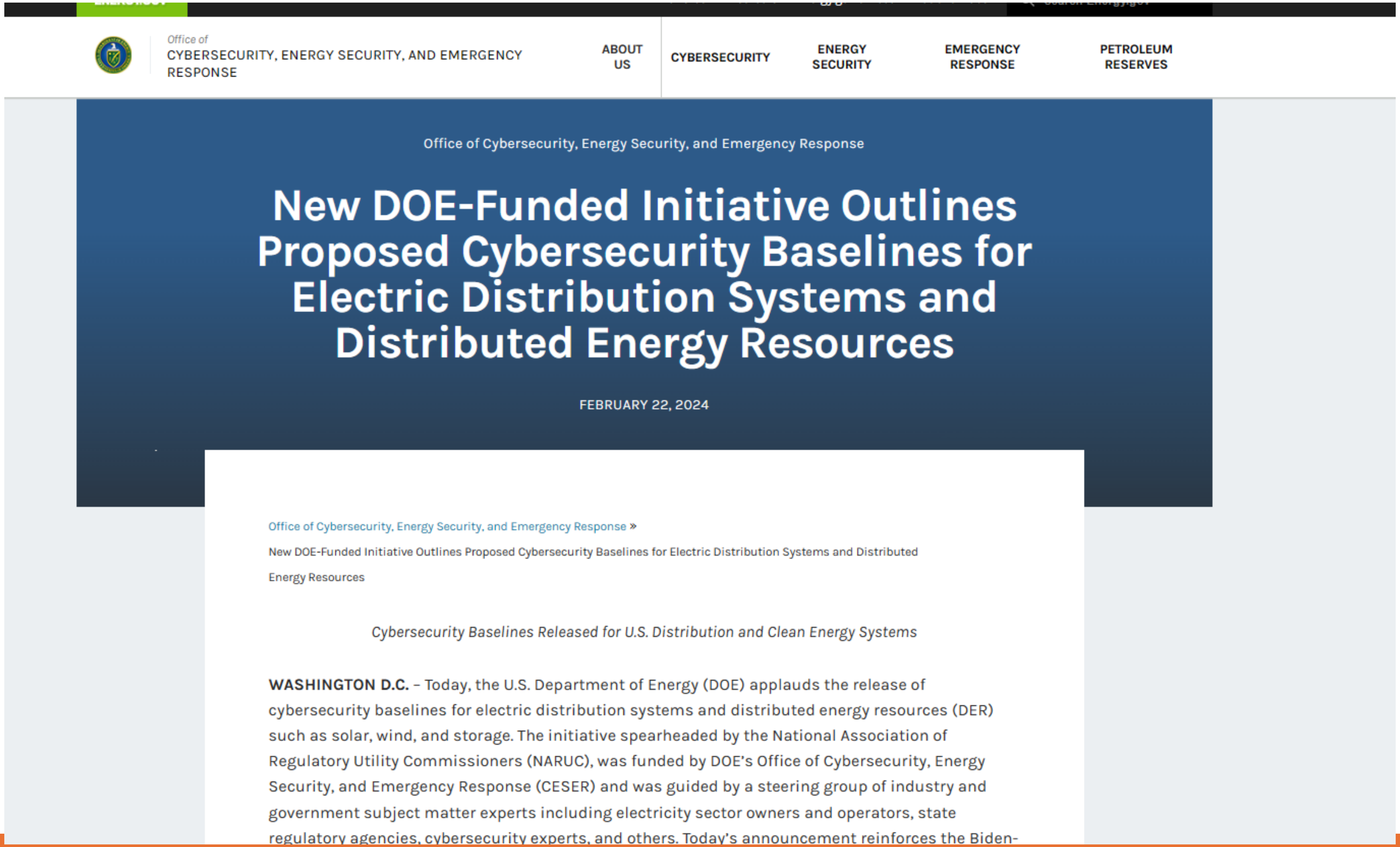
- **EPRI (Palo Alto, CA)** will develop and/or accelerate two communications standards to perform centralized management of authentication and authorization services in a zero-trust architecture.
- **Texas A&M University-Kingsville (Kingsville, TX)** will research, develop, and demonstrate a zero-trust authentication mechanism with post-quantum cryptography to reduce the cyber-physical security risks to DER devices and networks.
- **Kansas State University (Manhattan, KS)** will address the security vulnerabilities of existing standards by integrating authentication, secret key establishment, and encryption-based secure communication mechanisms with existing standards for reliable authentication and communication between smart grid nodes, inverters' gateways, and other grid-edge devices.

Important note: NO funding flows to the DNP Users Group

# DOE 2500 Project Work Plan - Preliminary

- In partnership with EPRI (prime and DER gateway)
- Completion of AMP device specification (core team development)
- Development of the AMP authority (commercial partner offering)
- Test procedures for SAv6 (core team development)
- Test procedures for AMP – Device and Authority (core team development)
- Development of the Protocol stack (commercial partner offering)
- Development of (extension to) test tool (commercial partner offering)
- Online testing – multi-vendor (core team development)
- Utility demonstration – multi-vendor (Salt River Project)
- Zero Trust Architecture – roadmap (core team development)

# DOE – Cybersecurity Baselines



Office of
CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Office of Cybersecurity, Energy Security, and Emergency Response

## New DOE-Funded Initiative Outlines Proposed Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources

FEBRUARY 22, 2024

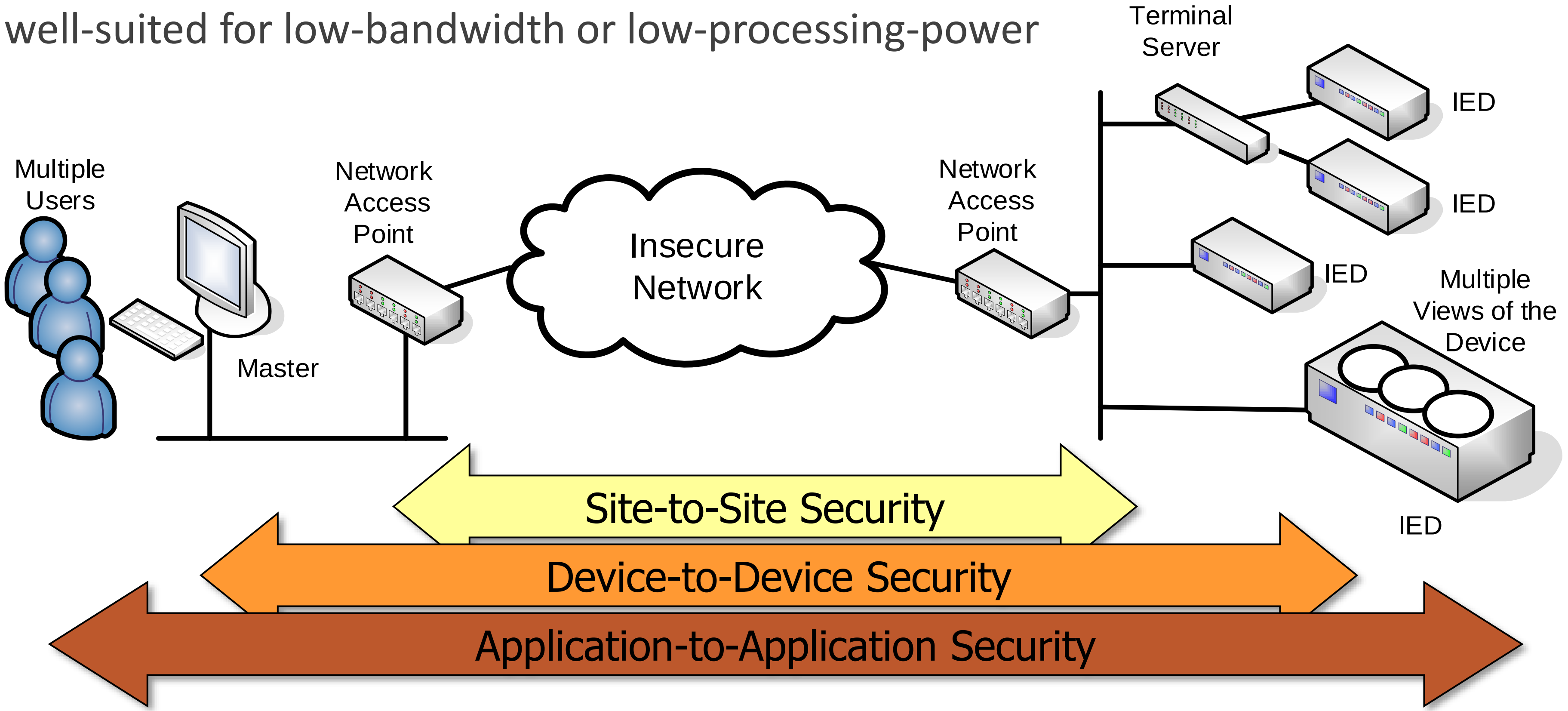
Office of Cybersecurity, Energy Security, and Emergency Response »
New DOE-Funded Initiative Outlines Proposed Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources

*Cybersecurity Baselines Released for U.S. Distribution and Clean Energy Systems*

**WASHINGTON D.C.** – Today, the U.S. Department of Energy (DOE) applauds the release of cybersecurity baselines for electric distribution systems and distributed energy resources (DER) such as solar, wind, and storage. The initiative spearheaded by the National Association of Regulatory Utility Commissioners (NARUC), was funded by DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and was guided by a steering group of industry and government subject matter experts including electricity sector owners and operators, state regulatory agencies, cybersecurity experts, and others. Today's announcement reinforces the Biden-

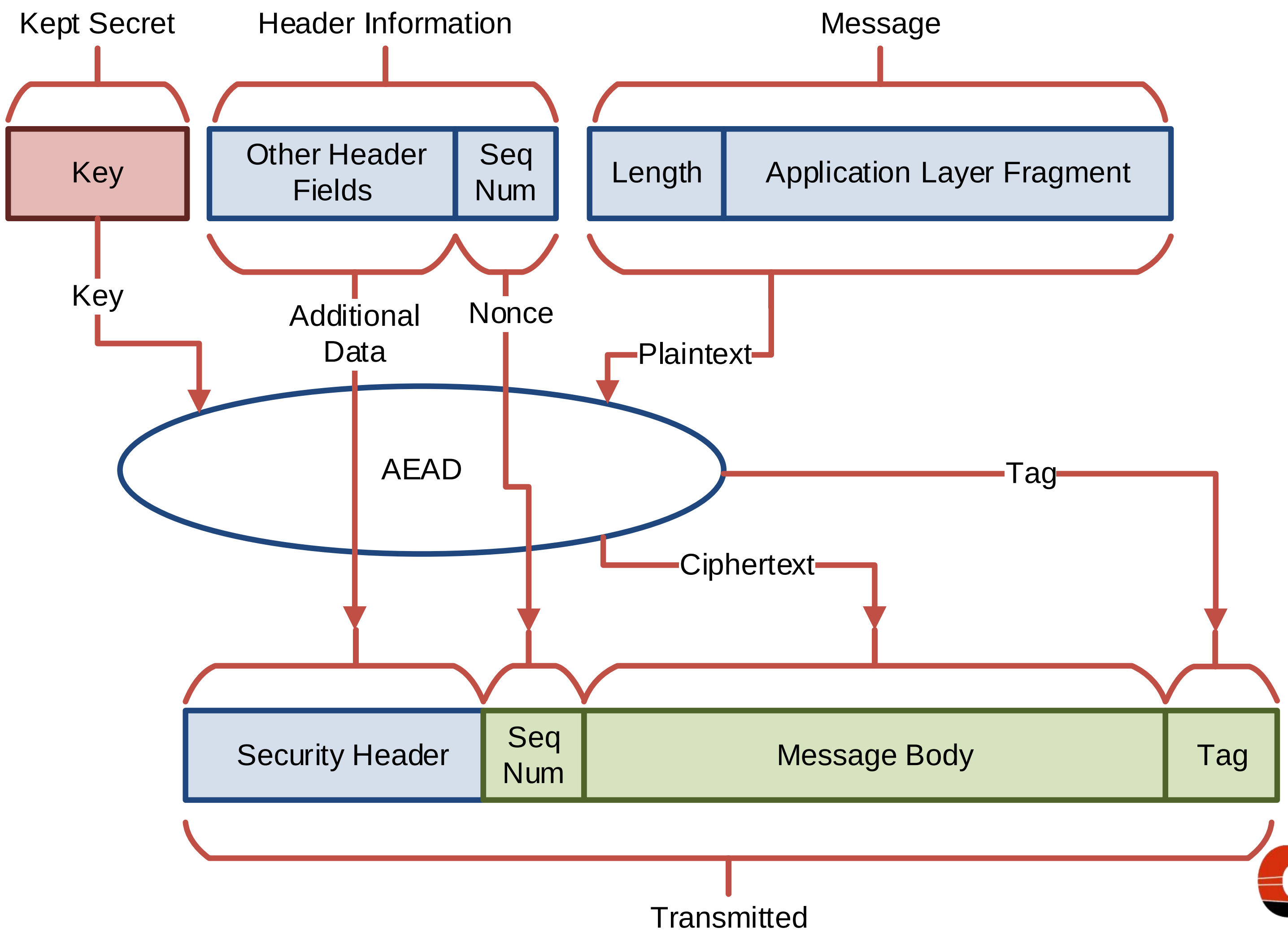
# Why Not Use TLS or IPSec?

- 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



# 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


Kept Secret
Header Information
Message
Key
Other Header Fields
Seq Num
Length
Application Layer Fragment
Key
Additional Data
Nonce
Plaintext
AEAD
Tag
Ciphertext
Security Header
Seq Num
Message Body
Tag
Transmitted