DISTRIBUTECH® CONFERENCE & EXHIBITION
FEBRUARY 9-11, 2016 + ORLANDO, FL
Owned & Produced By: PennWell
Official Publication of DistribuTECH: POWERGRID INTERNATIONAL
Supporting Publications: Electric Light&Power, WaterWorld, Renewable Energy World
Host Utility: OUC The Reliable One

Deploying Secure DNP3 (IEEE 1815) What You Need to Know

Technology Updates for Key Management

Joe Stevens

Marketing Manager

jstevens@trianglemicroworks.com

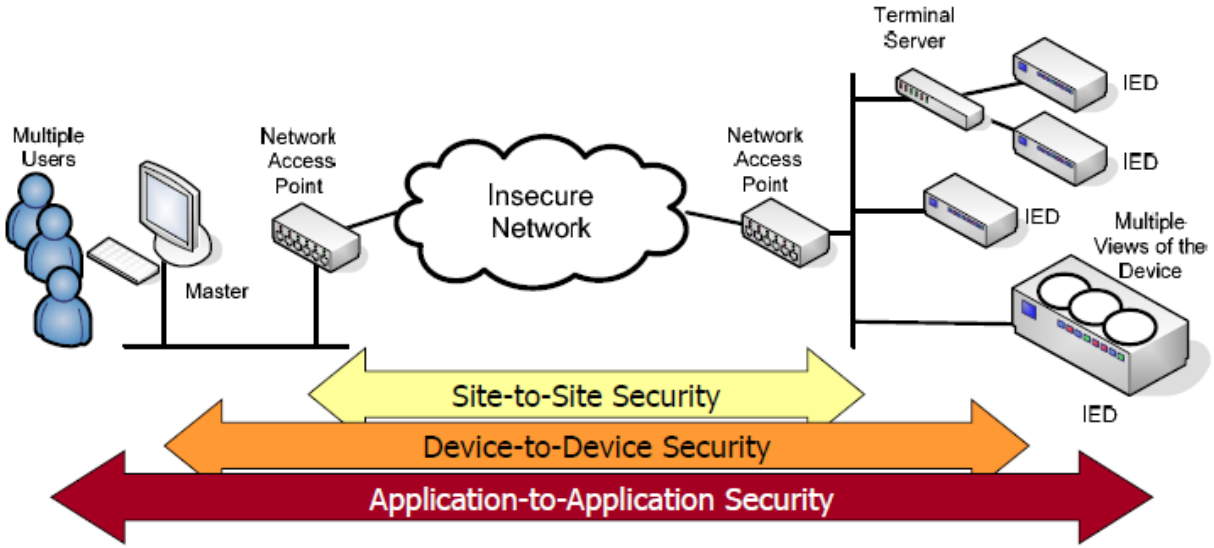
Triangle MicroWorks, Inc.
Solutions For Communication Protocol Development

Agenda

- **Why Secure Authentication?**
  - Benefits and Justification
- **Equipment Considerations**
  - Gateways/RTUs/Terminal Servers
- **Cyber Security Architecture**
  - Where Does SA Fit?
  - Multi-User Systems
  - Key Management
- **Technology Updates**
  - DNP Authority
  - DNP3 Key Management Protocol (DKMP)

Why Secure Authentication?

- User Authentication
  - Each critical operation is authenticated
  - Addresses threat of spoofing, modification, and replay
  - Not just about cyber-security but also operational reliability
- Legacy Support Requirements
  - Must have low overhead on devices
  - Support low bandwidth, serial, and IP networks
- TLS Encryption Can Be Added for DNP3 IP Networks



Benefits of DNP3 Secure Authentication

- **Increased security and reliability**
  - End to end cyber-security at the application layer goes beyond TLS or VPN
  - Can help meet authentication requirements of NERC CIP
  - Role Based Access Control addresses operational requirements of utilities

- **Can be implemented within existing infrastructure**
  - Security upgrade path without upgrading existing infrastructure or legacy devices

Equipment Considerations

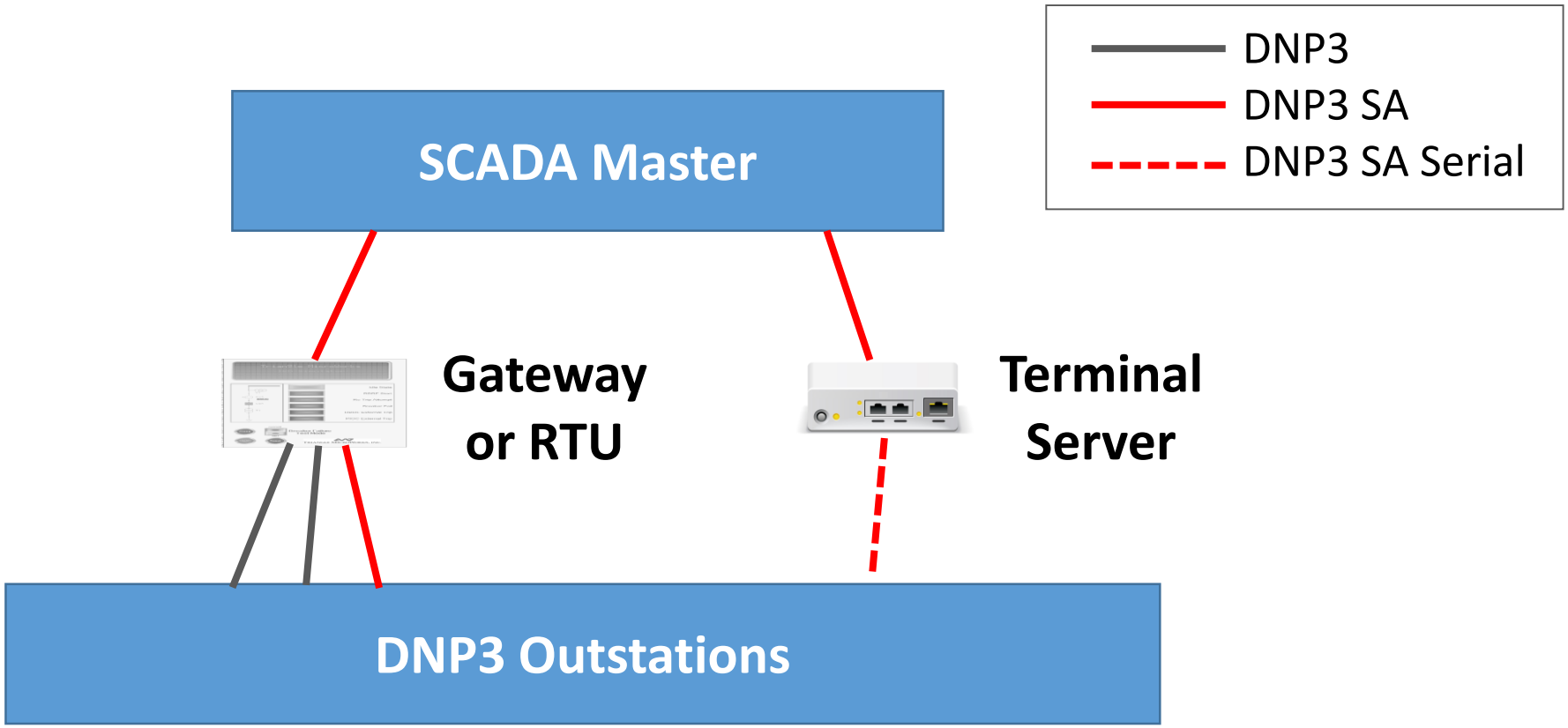
- **Are there devices that support Secure Authentication?**

  Short answer: Yes, a wide variety
  Long answer: Stop by the DNP booth downstairs!

- **What challenges are there for utilities and vendors?**

  - Determining a migration path to DNP3 SA
  - Operational adjustments (especially for role based access)
  - Planning for key management in the future
  - Vendors – not many challenges now after 10 years

Equipment Considerations



DNP3 SA to DNP3 without SA
Or mapping of DNP3 SA users

Supports IP to Serial and vice versa

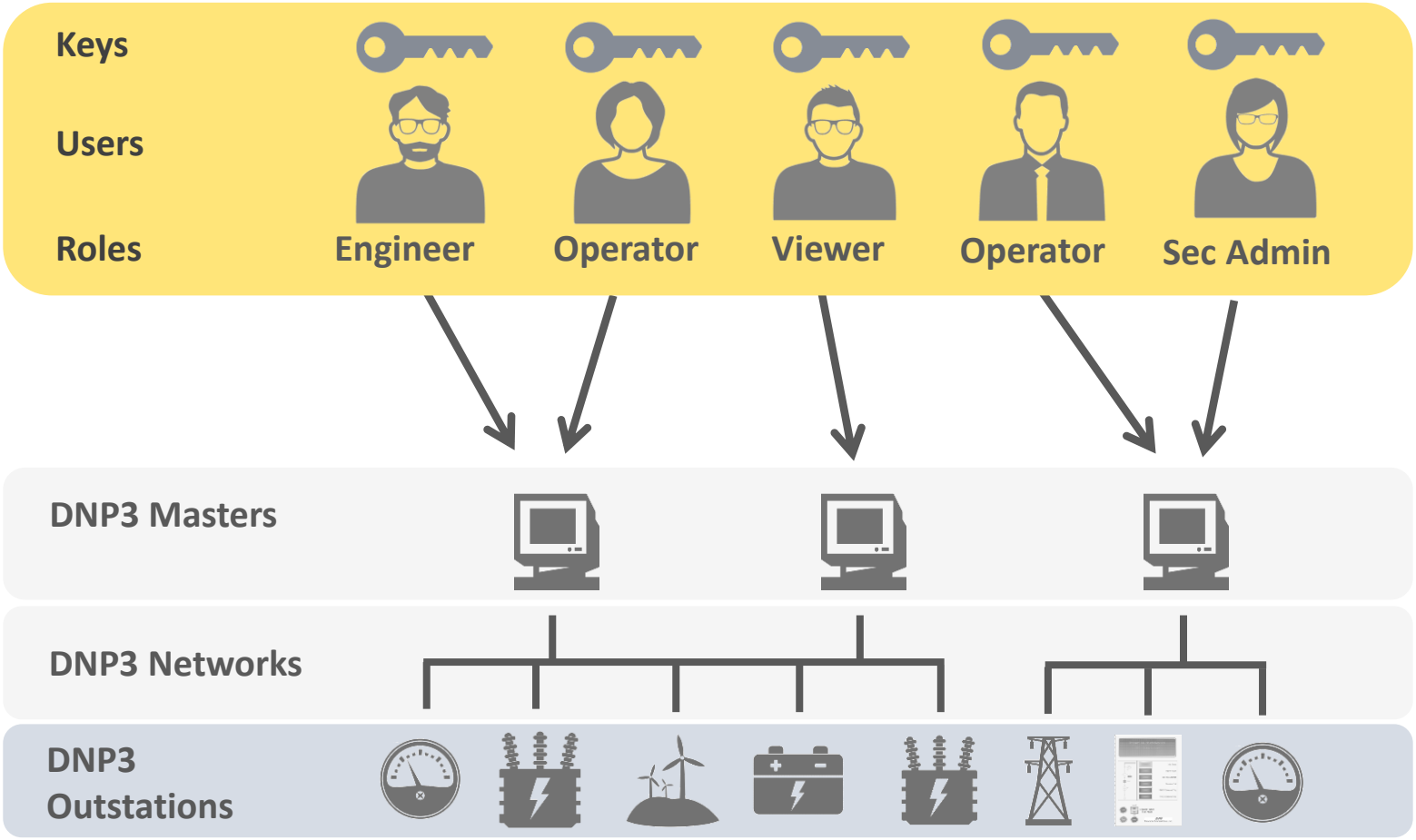
Multi-User Systems

- Role-Based Access Control (IEC 62351-8)
  - Each user has a role (Engineer, Operator, Security Admin)
- Privileges are based on the role
  - Standard roles have predefined privileges
  - Custom roles can be defined for each organization

		Privileges						
		View	Read	Reporting	File Read	File Write	Control	Security
User Roles	Viewer	✓		✓				
	Operator	✓	✓	✓			✓	
	Engineer	✓	✓	✓		✓		
	Security Admin	✓	✓			✓	✓	✓
	Security Auditor	✓	✓	✓	✓			

Multi-User Systems

- Users can be added to the system with specific roles
- Roles determine which privileges they have



Benefits of Role Based Access

- Operational Side
  - User access based on roles within organization
  - Greater reliability and safety by reducing risk of unintentional operations
  - Support for multiple organizations that share assets

- Security Aspects
  - Capability to log operations by DNP3 Master
  - Reduces risk of malicious attacks from within organization
  - Key disclosure has lower risk than a “single user” system

Key Management Dilemma

So many devices, users, keys…

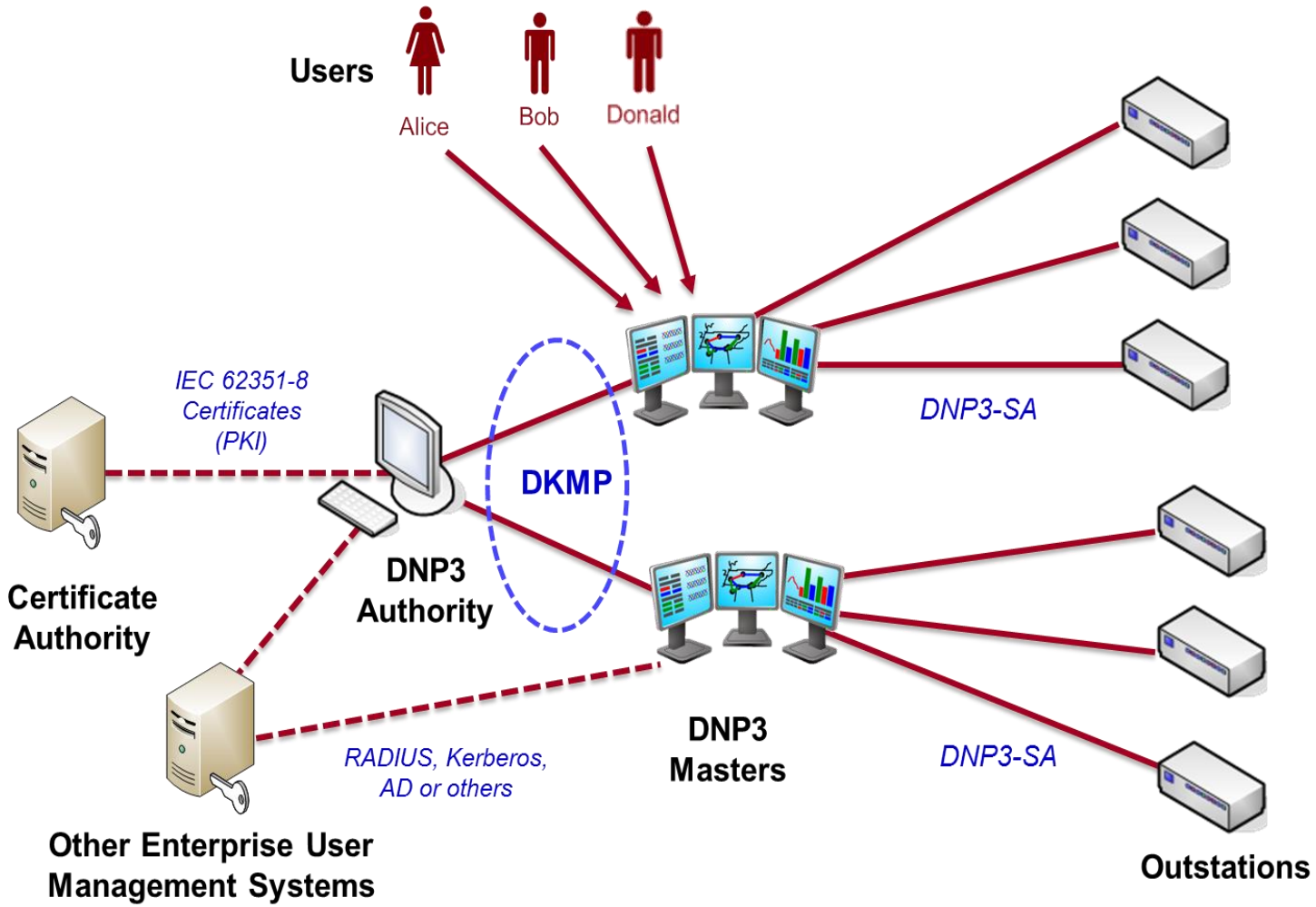
- How can users be added, removed, or modified?
- Who manages the updates?
- How do you update keys securely?
- How frequently do you need to update keys?
- What is the cost?
- Can this be automated?

Technology Updates

Updates to Secure Authentication

- IEEE Std™ 1815.1 Standard
- Security must evolve
- Backward compatibility is major goal
- Current objective: how will remote key management be standardized?
  - Much of the functionality exists in DNP3 now
  - DNP3 Authority evolving
  - Proposed key management interface for Masters

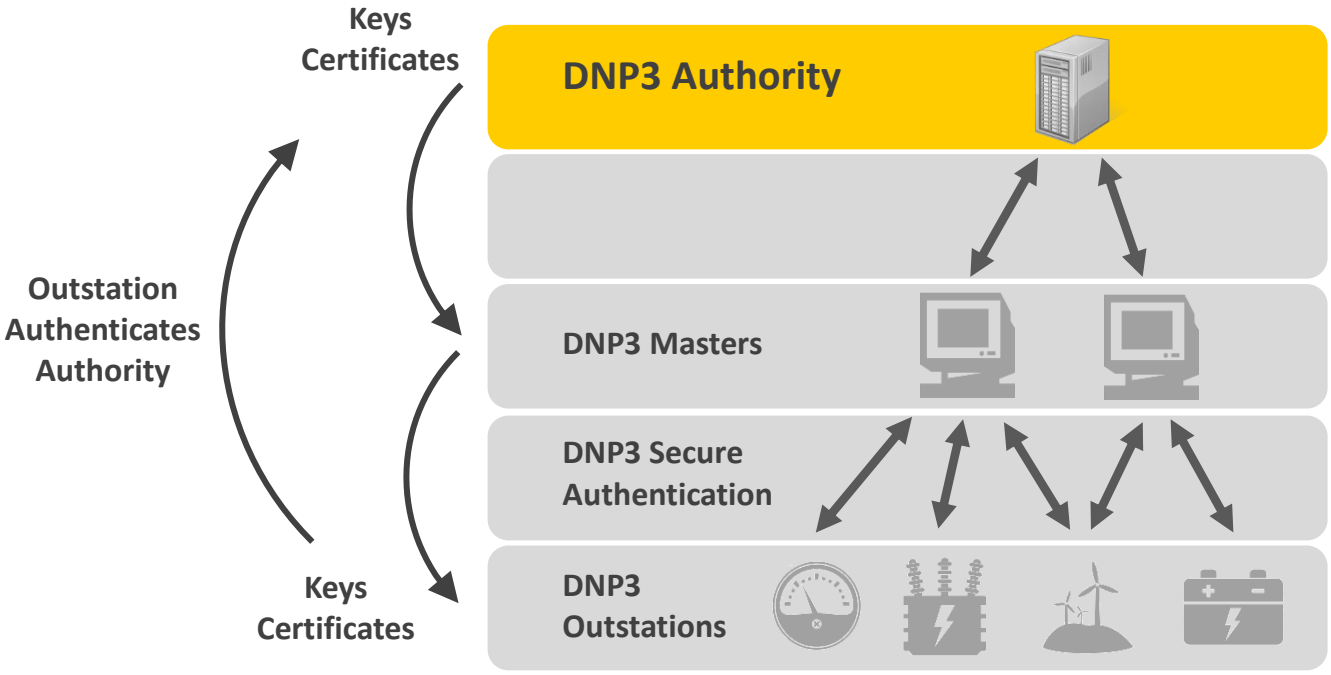
Cyber Security Architecture



DNP3 Authority

Central application across multiple DNP3 networks

- Interfaces to DNP3 Masters
- Adds, removes, and updates users
- Sends user keys/certificates to remote devices via Master

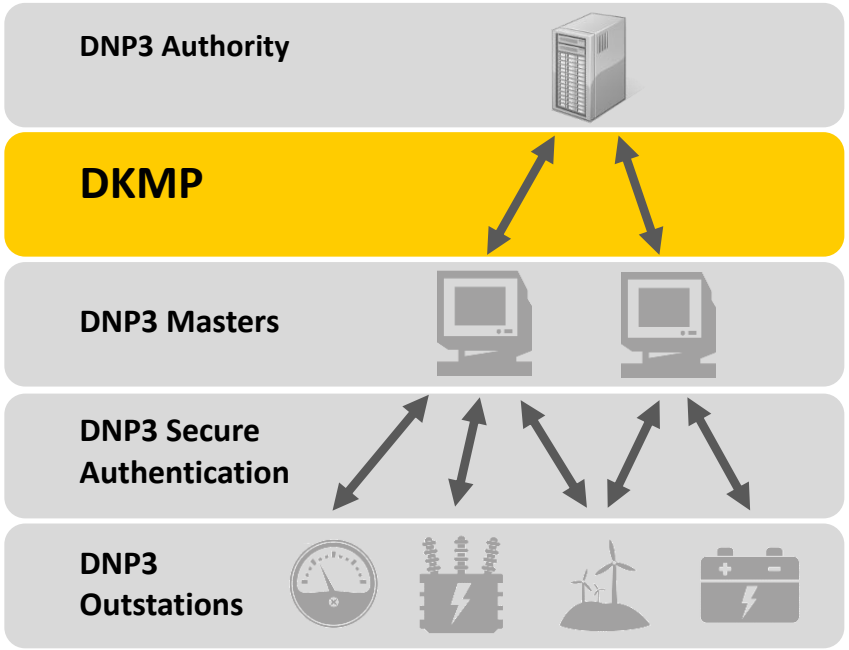


Enables remote key management

DNP3 Key Management Protocol (DKMP)

DKMP is a proposed specification*

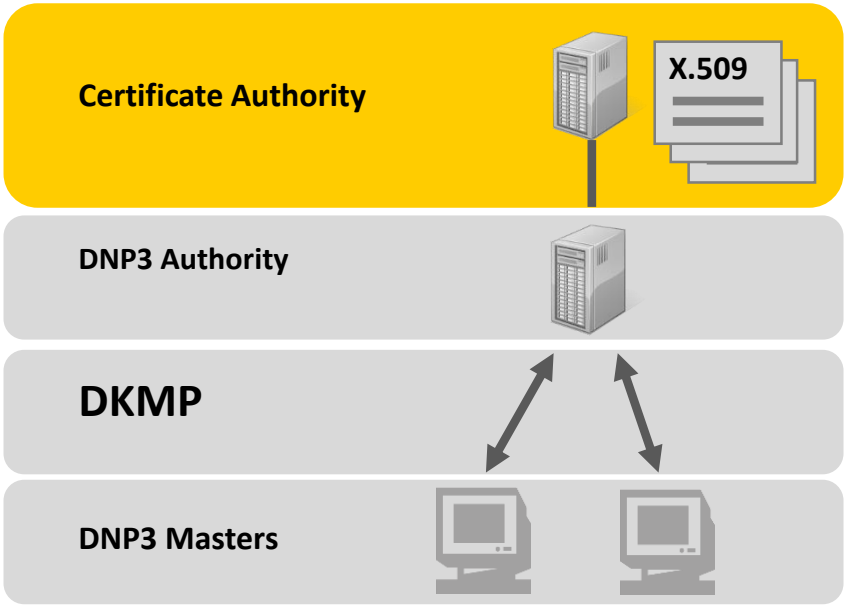
- Uses TLS over TCP Sockets
- Symmetric or asymmetric cryptography
- Synchronizes Users
- Updates Users
- Changes Keys



*Started as part of EPRI DNP3 demonstration in 2014

Certificate Authority

- Asymmetric cryptography
- Provides digitally signed certificates
- Interfaces to DNP3 Authority
- Supports X.509 certificates with IEC 62351-8 defined extensions:



X.509 Certificate

- User Role
- Lifetime of User Rights
- Operation (add, delete, change)

Why Key Management?

- Operational Benefits
  - Lower cost to update keys in remote devices
  - User access is based on operational requirements
  - Add and remove users as organization changes
  - Users are synched with central User Management System

- Security Benefits
  - Change keys quickly after an unintended key disclosure
  - Reduced risk of key disclosure versus manual distribution
  - Users can be removed as they leave the organization

DISTRIBUTECH®
CONFERENCE & EXHIBITION
FEBRUARY 9-11, 2016 + ORLANDO, FL
Owned & Produced By: PennWell
Official Publication of DistribuTECH: POWERGRID INTERNATIONAL
Supporting Publications: Electric Light & Power, WaterWorld, Renewable Energy World
Host Utility: OUC The Reliable One

Deploying Secure DNP3 (IEEE 1815) What You Need to Know

Joe Stevens

Marketing Manager

Triangle MicroWorks

jstevens@TriangleMicroWorks.com