



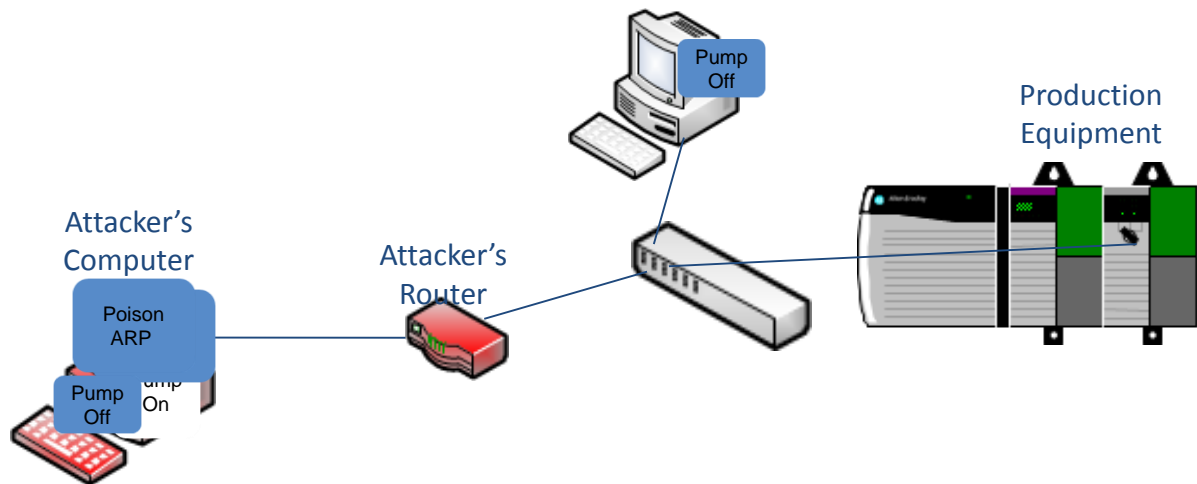
CIP Security Phase 1

Secure Transport for EtherNet/IP

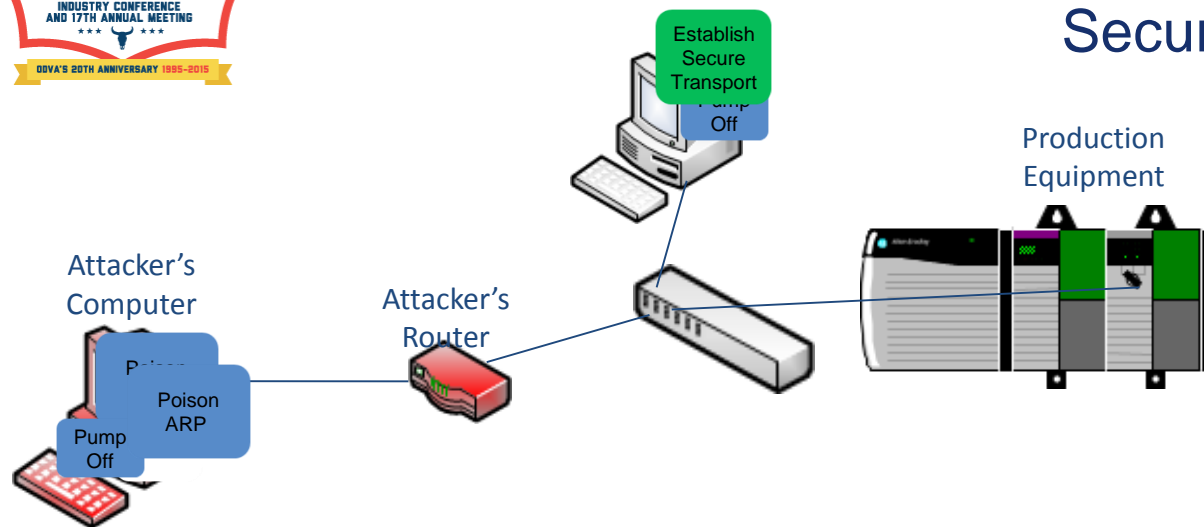
Brian Batke, Rockwell Automation
Dennis Dubé, Schneider Electric
Joakim Wiberg, HMS Industrial Networks

October 14, 2015

The Need for a Secure Transport



Secure Transport Solution



CIP Security Goals

- ***Reject data that has been altered (integrity)***
- ***Reject messages sent by untrusted entities (authenticity)***
- ***Reject actions that are not allowed (authorization, phase 2)***



Specification Enhancements for CIP Security

Specification Enhancements for CIP Security™	General Description	Technical Description
Device Hardening	EtherNet/IP product hardening requirements and recommendations	Protection Mode attribute to Identity Object. Recently updated to include Implicit and Explicit modes
The CIP Networks Library 2015 PC2	Secure communications between <u>EtherNet/IP</u> endpoints: data integrity, data confidentiality, and device authenticity	EtherNet / IP over TLS for UCMM and Class3 EtherNet / IP over DTLS for Class 0/1 Security is only assured on Ethernet
The CIP Networks Library 2017+	Secure <u>end-to-end</u> communications between <u>CIP</u> endpoints: data integrity, device and <u>user</u> authenticity	CIP enhancement to support user and device authentication along with device access policy enforcement (authorization)



CIP Security Features

Security Properties	CIP Security™ (2015)	CIP Security™ (2017+)
Device Authentication	√ (Ethernet device)	√ (CIP device)
Device Trust Model	Broad (group(s) of trusted devices)	Narrow (individual trusted device or app)
Device Identity	√ (PSK or X.509 Certificate)	√ (TBD)
Integrity	√ (Ethernet transport layer)	√ (CIP application layer)
Confidentiality	√	√ (TBD)
User Authentication		√
Change Detection (Audit)		√ (CIP device)
Policy Enforcement (Authorization)		√



CIP Security Profiles

EtherNet/IP Integrity Profile :

Provides device authentication and data integrity of packets on Ethernet networks.

EtherNet/IP Confidentiality Profile :

Provides confidentiality to data in transit

(Adds Confidentiality to EtherNet/IP Integrity profile)

CIP Authorization Profile:

Provides user & device authentication and device access policy enforcement (authorization)

CIP Integrity Profile:

Provides end to end data integrity at the CIP application layer

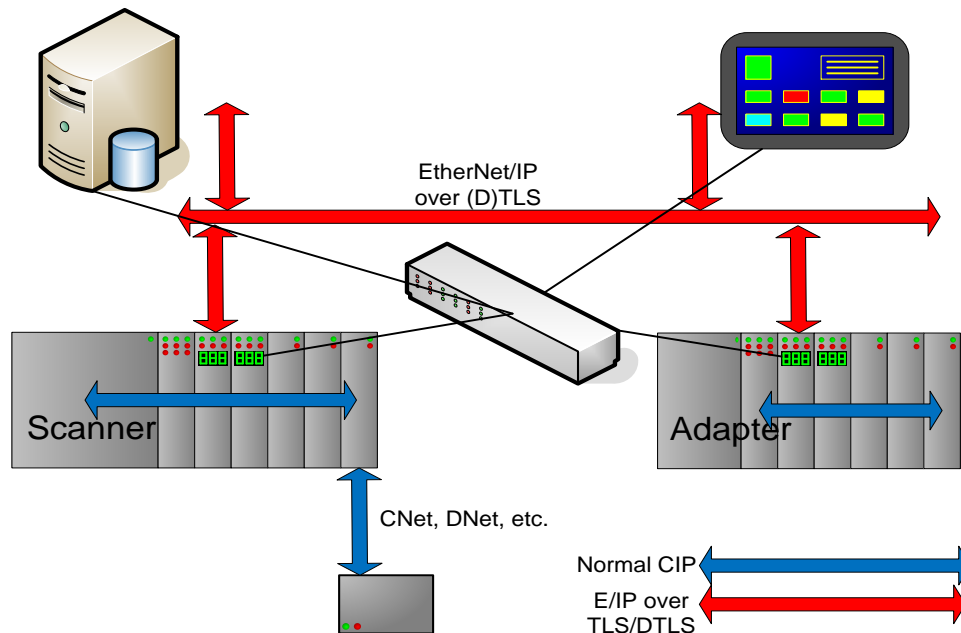
(Adds CIP Integrity to the CIP Authorization profile)



Phase 1 Solution Summary

- TLS (TCP) and DTLS (UDP) provide the secure transport
 - Same approach as HTTPS: HTTPS = HTTP over SSL/TLS
 - Secure EtherNet/IP = EtherNet/IP over TLS and DTLS
 - Same EtherNet/IP, but over a secure transport

CIP Security P1: EtherNet/IP over TLS/DTLS





Phase 1 Solution Summary

- What is TLS?
 - “Transport Layer Security”
 - Defined via RFCs: RFC 5246 for TLS; RFC 6347 for DTLS
 - Related RFCs for X.509 certificates, cipher suite definitions, etc.
 - Standard protocol, widely used to secure Internet traffic

Bottom line: We don't have to invent the secure transport

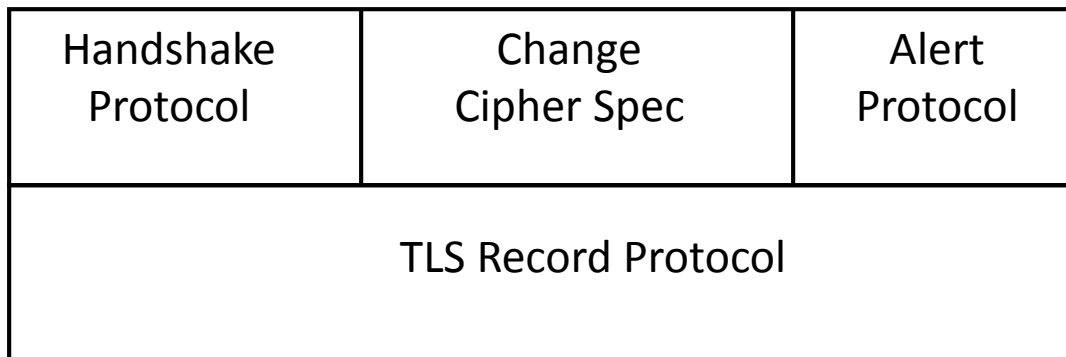
We just use it for EtherNet/IP

Establish a session

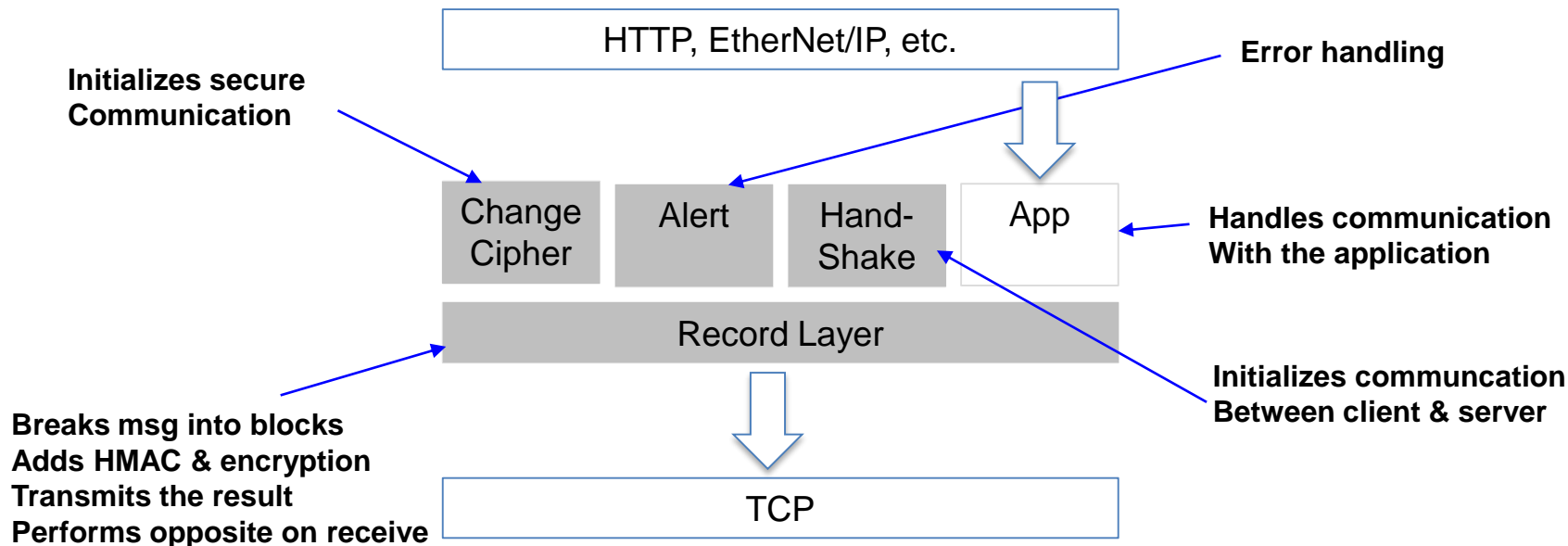
- Agree on algorithms, share secrets, perform authentication

Transfer application data

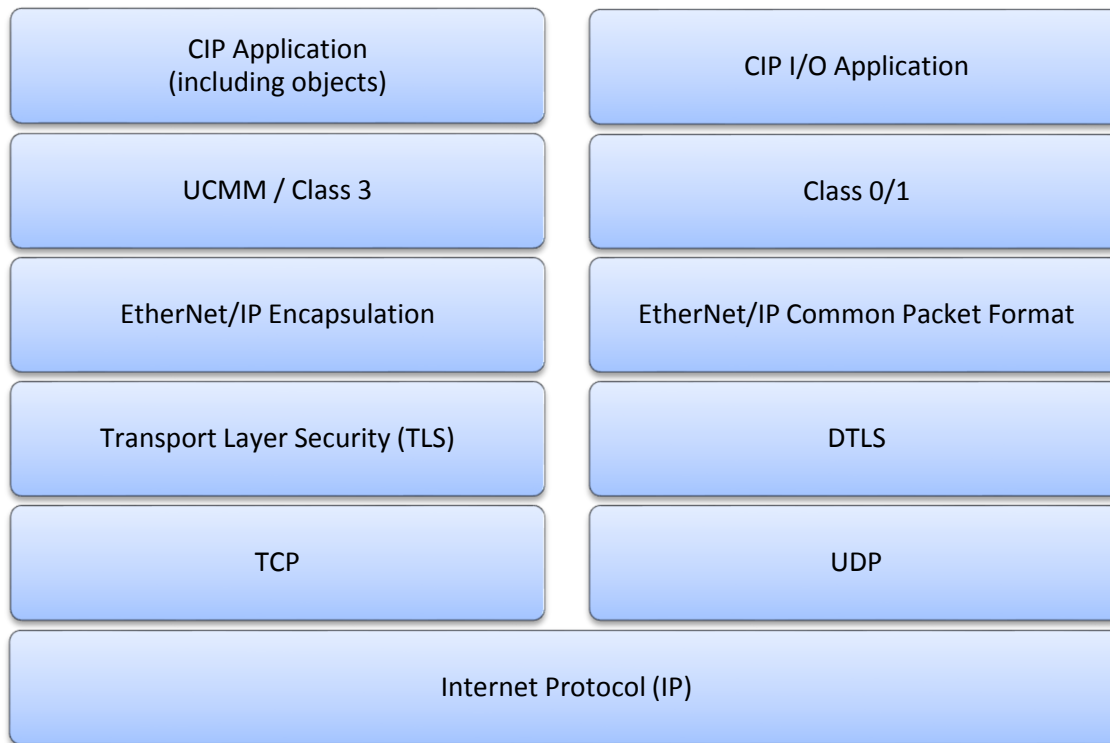
- Ensure privacy and integrity



TLS Architecture




CIP Security Layers



CIP Security Capabilities


- Only trusted entities (device or s/w app) able to connect. Two trust options:
 - Pre-Shared Keys (PSK), configured in originator and target
 - X.509 Certificates, with common root authority
 - In both cases, both originator and target verified
- Message integrity and authenticity
 - Provided by HMAC on (D)TLS packets.
 - Includes anti-replay
- Optional message encryption
 - Will be a user choice (performance impact)



Prevent
untrusted
comms

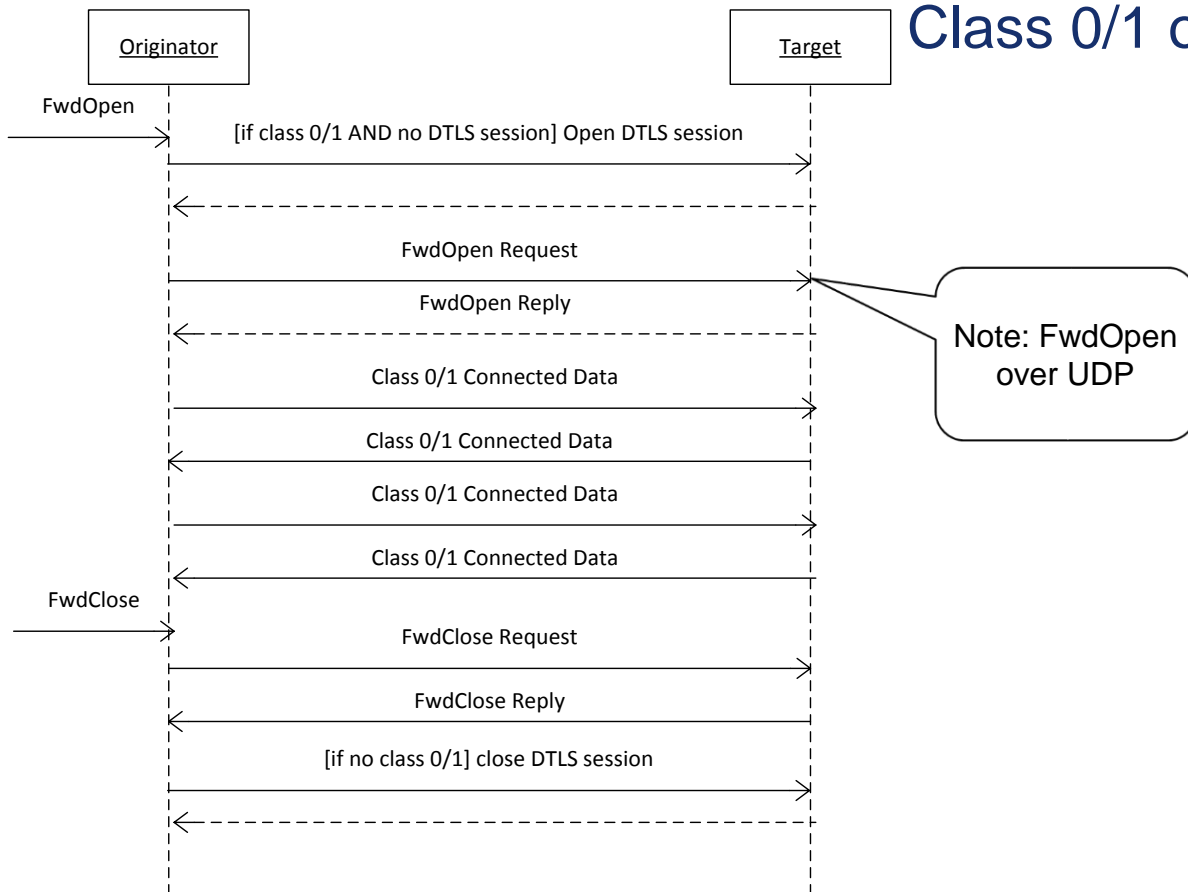


Prevent
msg
tampering



Prevent
eaves-
dropping

Class 0/1 over DTLS





Volume 8 Content

Chapter 1: Introduction

Chapter 2: <currently empty, expected to be CIP Security>

Chapter 3: EtherNet/IP Security

Chapter 4: Configuration and Commissioning

Chapter 5: Object Library

Chapter 6: Security Profiles

Chapter 7: <currently empty, expected to be EDS Files>

Chapter 8: Certificate Management



Volume 8 Content

- Behavior of EtherNet/IP over TLS and DTLS (Chapter 3)
 - New port number (2221 for both TCP and UDP, registered with IANA)
 - Required (D)TLS cipher suites
 - New CPF message for FwdOpen over UDP (in Volume 2, Chapter 2)
 - Originator and target behavior with respect to (D)TLS
 - Multiple connections, sequence number rollover, etc.



Cipher Suites

Cipher Suite	Description
TLS_RSA_WITH_NULL_SHA256	RSA for key exchange; null encryption; SHA256 for message integrity. Encryption not provided.
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA for key exchange. AES 128 for message encryption, SHA256 for message integrity.
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA for key exchange. AES 256 for message encryption, SHA256 for message integrity.
TLS_ECDHE_ECDSA_WITH_NULL_SHA	ECDHE_ECDSA for key exchange; null encryption; SHA1 for message integrity. Encryption not provided.
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE_ECDSA for key exchange. AES 128 for message encryption, SHA256 for message integrity.
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE_ECDSA for key exchange. AES 256 for message encryption, SHA256 for message integrity.
TLS_ECDHE_PSK_WITH_NULL_SHA256	ECDHE in conjunction with PSK for key exchange; null encryption; SHA256 for message integrity. Encryption not provided.
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256	ECDHE in conjunction with PSK for key exchange. AES 128 for message encryption, SHA256 for message integrity.



CIP Security Object

- Exclusivity during commissioning

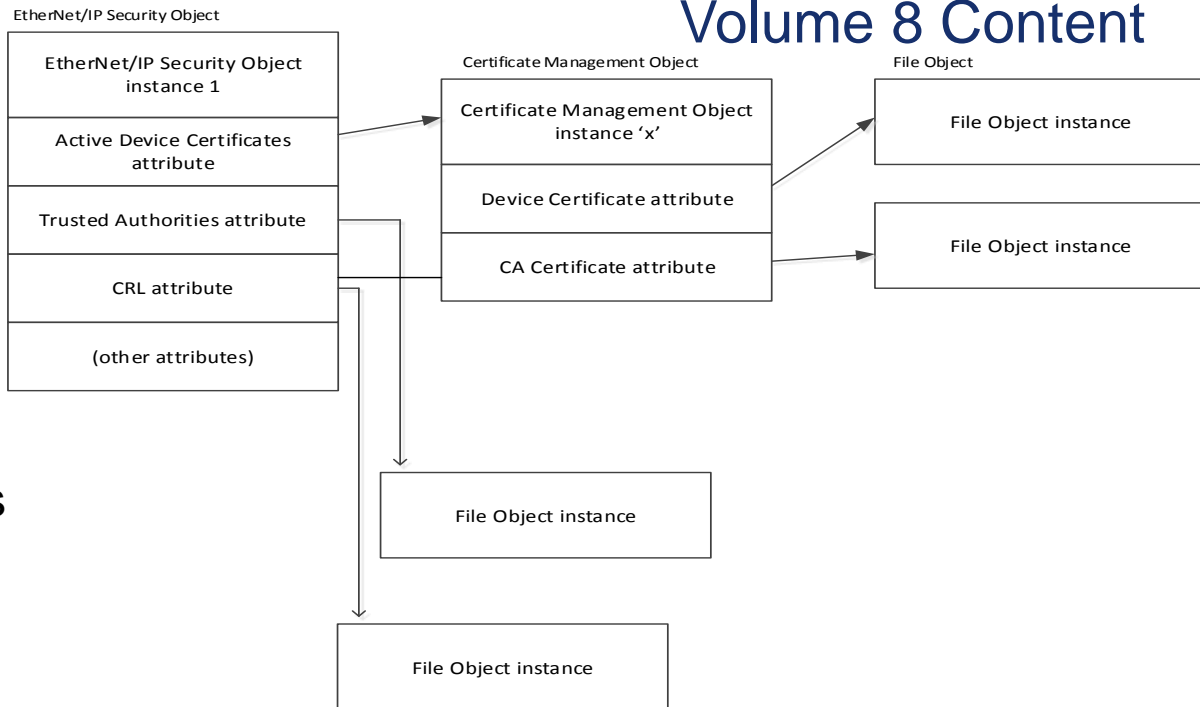
EtherNet/IP Security Object

- Configuration of TLS/DTLS related settings

Certificate Management Object

- Interface to get/set certificate and related files

Volume 8 Content





Volume 8 Content

- Certificate management requirements / recommendations
 - Vendor certificate recommended (802.1AR)
 - Self-signed default certificate if no vendor cert
 - Key generation and storage considerations
- CIP Security profiles
 - Defined groupings of capabilities
 - Will drive conformance test



... But will it work?

- Several vendors have prototype implementations
 - UCMM / Class 3 over TLS
 - Class 0 / 1 over DTLS (partial implementation)
- Possibility of multi-vendor prototype interop event
 - Tentative
 - More participants welcome!



Next steps

CIP Security Phase “1.5”

- ***Certificate enrollment via standard protocol (EST required, SCEP optional)***
- ***Multiple certificate support***
- ***Investigate secure multicast support***

CIP Security “Phase 2”

- ***CIP level authentication and authorization***
- ***Users and devices***
- ***Will require further input and scoping with ODVA Security Task Force***



THANK YOU