**Ethernet Security Specification**

Version 1.00

Version Date: December 6, 2018

UNCONTROLLED COPY IF PRINTED

**FORD CONFIDENTIAL**

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created/Modified By** | **Notes** |
| 12/06/2018 | 1.0 | Justin Mendenhall/jmenden2 | Initial Release Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Introduction 4](#_Toc514157349)

[1.1 Purpose 4](#_Toc514157350)

[1.2 Terminology and Abbreviations 4](#_Toc514157351)

# Introduction

## Purpose

The main goal of this document is to provide an overview of security features in the system. The document expects to capture the overarching goals for Security and the security feature requirements for meeting those goals. It focuses on commonalities of the different features and on points of interaction between the features. Specific security features that are native to the platform are distinguished from those that would need additional implementation consideration.

To understand the functional/behavioral level detail for each security feature, please refer to the individual functional specification for that function.

## Terminology and Abbreviations

| **Term** | **Description** |
| --- | --- |
| AES | Advanced Encryption Standard |
| RNG | Random Number Generator |
| CA | Certificate Authority |
| CRL | Certificate Revocation List |
| EOL | Manufacturing End of Line |
| IPC | Inter-processor Communication (between CCPU/VMCU) |
| CCPU | Client CPU (LS1043A core running high level functions and cloud communication |
| VMCU | Vehicle Management CPU (MPC5748G running CAN Gateway functionality |
| IBD/OBD | Inbound/Outbound Diagnostics (over IPC) |
| RTC | Real-Time Clock |
| Logical Attack | An attack involving an unintended hole in the functioning of the system such as a security hole that allows an attacker to circumvent intended security controls. |
| Physical Attack | An attack requiring physical access to the device and manipulating internal operations to cause it to perform unintended operations. |
| Administrative Attack | An attack against the user or documented processes of how things should operate. Classic examples are phishing attacks or social engineering. |

# Feature Design Requirements

## Architecture

## Goals

Secure Communication – Ethernet security mechanisms must ensure that sensitive data is not disclosed or tampered with. All Ethernet traffic should be authenticated or negotiated over authenticated connections prior to transmission. SOA based traffic shall be authenticated using TLS.

## Non-Goals

# Requirements

## Functional Requirements

### Module/Device Authentication and Authorization

**Requirement Text:** All modules and devices shall authenticate themselves against SOA and the ECG. Port transmission speed shall be reduced while the connected module is not authenticated. The port routing table shall only route to the ECG while the module is pending authentication. Authentication and Authorization shall take place over a secure communication channel. This channel shall use bi-directional TLS 1.2 with approved cipher suites.

TLS certificates shall use the X.509 format with RSA-2048 key length and the sha256 with RSA Encryption Signature Algorithm.

When a module contains multiple microcontrollers/components with Ethernet interfaces that are connected to a Ethernet switch that resides within the same module **and** devices cannot be added or removed from that switch:

* These modules do not need to be authenticated until they transmit traffic to the ECG or to a non-resident module.
* The routing table shall not permit traffic to be sent to non-residents modules, with the exception of the ECG.
* Internal port speed is not required to be limited.

**Definition:** Approved TLS cipher suites:

* + - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P384
    - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256
    - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P384
    - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256

**Requirement Author:** Justin Mendenhall

**Goal: To prevent unapproved or unauthorized devices from communicating on the network and to prevent credentials from being compromised while they are transmitted.**

**Rationale:** Credentials used to authenticate a module to the network need to be protected when in transit. TLS 1.2 used in combination with approved cipher suites provide an appropriate level of protection.

**Verification Type:** DV

### Message Security

**Requirement Text:** All Ethernet traffic shall be authenticated or negotiated over authenticated connections prior to transmission.

If the message does not contain credentials, sensitive data, or confidential data, the cipher suite may be changed to a cipher that does not encrypt the primary payload.

Traffic internal to a module, where devices or microcontrollers cannot be added or removed from the internal switch, do not require authentication.

**Definition:** Approved TLS cipher suites for sensitive or confidential messages:

* + - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P384
    - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256
    - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P384
    - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256

**Requirement Author:** Justin Mendenhall

**Goal: To prevent unapproved or unauthorized devices from communicating on the network and to prevent credentials from being compromised while they are transmitted.**

**Rationale:** Message receipients must be able to authenticate the message and verify that it was sent from a known and trusted source. Messages containing sensitive data shall emply appropriate controls to protect to confidentiality and integrity of that message.

**Verification Type:** DV

### Key Management

**Requirement Text:** The module shall store private keys and symmetric keys in a secure tamper resistant memory location that does not permit unauthorized entities to read from. Public keys shall be stored in a protected memory location that is read-only.

Refer to Key Provisioning specification for obtaining keys.

**Definition:**

**Requirement Author:** Justin Mendenhall

**Goal: To prevent keys from being compromised.**

**Rationale:** Keys and credentials need to be protected. Modifying or compromising these keys can permit other devices to access the network, impersonate devices, and send malicious or malformed data.

**Verification Type:** DV

### Address Resolution Protocol (ARP)

**Requirement Text:** ARP shall not be active during normal operation modes. Special operation modes can only be activated via secure DIDs using service $27. Activation of ARP shall be logged and shall increment an event counter.

ARP/CAM tables shall not be modified during normal operation.

**Definition:**

**Requirement Author:** Justin Mendenhall

**Goal: Prevent unauthorized messages from being forwarded and to prevent tampering of ARP tables.**

**Rationale:** Limiting when ARP is active reduces the window when new modules or devices can be added to the network. It also reduces the chance of the ARP/CAM tables being modified and traffic being redirected (better refered to as ARP cache poisoning).

**Verification Type:** DV

### Dynamic Host Configuration Protocol (DHCP)

**Requirement Text:** DHCP shall only be active during special operation modes. Special operation modes can only be activated via secure DIDs using service $27. Activation of DHCP shall be logged and shall increment an event counter.

**Definition:** Special operation modes are limited to manufacturing and module replacement.

**Requirement Author:** Justin Mendenhall

**Goal: To prevent unauthorized devices from being added to the network, to prevent modules from impersonating an authorized device, and to prevent man in the middle scenarios**

**Rationale:** Limiting when DHCP is active reduces the window when new modules or devices can be added to the network.

**Verification Type:** DV

### Protocol Support

**Requirement Text:** Protocols not stated or referenced in this document shall not be supported. If a protocol is required, it shall be reviewed by the Ford Security team for approval.

**Definition:**

**Requirement Author:** Justin Mendenhall

**Goal: To prevent use of unauthorized protocols**

**Rationale:** Limiting what protocols can be used reduces potential attack attack vectors.

**Verification Type:** DV

## Process Requirements

### Fuzz Testing

**Requirement Text:** The Ethernet Interface shall undergo fuzz testing using a tool approved by Ford. Fuzzing shall include networking protocols that are used over Ethernet. The system shall not become unresponsive, shall not act abnormally, and shall remain in its default state.

**Definition:** Ford Approved Tools: Defensics Networking test suites

**Requirement Author:** Justin Mendenhall

**Goal: To prevent the system from performing abnormally or becoming unresponsive**

**Rationale:** Fuzz Testing provides random data to the inputs of a system. This technique is useful on all systems especially systems with inputs presented to it by various interfaces. Fuzz Testing is also useful testing the stability of systems.

**Verification Type:** DV

### Port/Service Scan

**Requirement Text:** The system containing a Ethernet Interface shall undergo a port scan to identify available services using a tool approved by Ford. Only services approved by Ford shall be identified. Un-approved services shall be removed from the system.

**Definition:** Approved tools: nmap, nessus

**Requirement Author:** Justin Mendenhall

**Goal: To identify available services and ports resident on the system**

**Rationale:** Unapproved ports or services may provide a backdoor into the system or result in the system operating in either a reduced capacticy or in an unitended manner.

**Verification Type:** DV