

Connected-X Cybersecurity

**Key Material Requirements**

DRAFT DOCUMENT

Version 0.1

Version Date: February 1, 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** |
| 1/30/2018 | .1 | Joby Jester | Initial Version |

**Table of Contents**

[1 Introduction 4](#_Toc505339442)

[1.1 Executive Summary 4](#_Toc505339443)

[1.2 Purpose of Document 4](#_Toc505339444)

[1.3 References 4](#_Toc505339445)

[1.4 Terminology and Abbreviations 4](#_Toc505339446)

[2 Feature Design Requirements 5](#_Toc505339447)

[2.1 Goals 5](#_Toc505339448)

[2.2 Design Dependencies 5](#_Toc505339449)

[2.2.1 Key Storage 5](#_Toc505339450)

[2.2.2 Certificate Storage 5](#_Toc505339451)

[2.3 Keys, Certs, and Uses 5](#_Toc505339452)

[2.3.1 Cloud/SDN Connectivity 5](#_Toc505339453)

[2.3.2 ECU Diagnostics 6](#_Toc505339454)

[2.3.3 Software Installation 6](#_Toc505339455)

[2.4 Additional Details 6](#_Toc505339456)

[2.4.1 ESN 6](#_Toc505339457)

[2.4.2 Processor ID 6](#_Toc505339458)

# Introduction

## Executive Summary

As part of the development process, vendors must comply with several requirements including the SyncP, Software Signing, and Supplier Feed Specifications. The need to outline key material and certificates is part of the initial discussions with any module supplier. The goal is to create a baseline document containing the keys and certificates expected for any Ford module that interacts in a connected vehicle ecosystem.

## Purpose of Document

The purpose of this document is to outline several keys and certificates and how they interact with the Ford SDN (Au). This document is module agnostic and shall be considered a general guide unless specified as a requirement.

The document will focus on the following areas:

* Key Types and Usage
* ESN definitions
* Certificates and Usage

## References

This section contains references to documents, which affect the requirements presented in this requirement specification.

| **Reference Title** | **Document Location** |
| --- | --- |
| A51\_Supplier\_Feed\_Specification(Multiple) | VSEM |
| S13a\_SyncP\_Functional | VSEM |
| 3GPP TS 23.003 | <http://www.3gpp.org/ftp/Specs/html-info/23003.htm> |

## Terminology and Abbreviations

| **Term** | **Description** |
| --- | --- |
| AP | Application Processor. Can also be referred to as CCPU or SoC |
| CA | Certificate authority or certification authority (CA) is an entity that issues digital certificates. See <https://en.wikipedia.org/wiki/Certificate_authority> for more details. |
| CP | CAN-Facing Processor. Can also be referred to as VMCU or IoC |
| ESN | Electronic Serial Number is a unique per module ASCII identifier. |
| IMEI | International Mobile Station Equipment Identity that is used to identify valid satellite phone devices.  See <http://en.wikipedia.org/wiki/International_Mobile_Station_Equipment_Identity> for more details |
| OpenSSL | Open source implementation of the SSL/TLS protocols, this tool also provides general CA, SMIME, etc. See OpenSSL man page for additional details. |
| PKCS#7 | Defined in RFC 2315, used to sign/encrypt messages within a PKI infrastructure, and formed the basis for SMIME security. See <http://en.wikipedia.org/wiki/PKCS> for more details and definitions. |
| SDN | “Service Delivery Network” is Ford Connected Services ecosystem hosted at a cloud provider that provides infrastructure for all Ford’s global connected vehicle programs. |
| SyncP | Proprietary Ford protocol used for encryption of messages  Refer to S13a and S13b for implementation details |
| X.509 | Format of certificates used for key packages. See <http://en.wikipedia.org/wiki/X.509> for more details and definitions. |

# **Feature Design Requirements**

## Goals

* The main goal of this document is to outline the common keys used by Ford ECUs that communicate with the SDN.
* This document should be a baseline and is architecture independent.
* This document does not cover the format of items discussed in the module’s A51 Supplier Feed specification.

## Design Dependencies

### Key Storage

In order to secure communication between ECUs, SDN, and (if applicable) final customers, a comprehensive key infrastructure shall be developed. The primary communication between Ford systems and the connected vehicle ecosystem is a proprietary protocol known as SyncP. SyncP is a message level encryption scheme utilizing a shared secret key between the module and cloud.

As a base requirement, all private keys stored on device shall be stored in HSM or other secure storage. Ford Motor Company shall solely own and control all keys used in conjunction with the system unless otherwise stated.

Operations involving keys stored in the secure key storage (encryption, decryption, signature validation, etc.) shall be fully contained within the secure key storage at rest and, where practical, shall be protected via mechanisms such as ARM Trust Zone during usage. If cryptographic functions are hosted outside of secure key storage, device shall not allow keys/certs to remain in RAM for more than **100**ms.

### Certificate Storage

Certificates utilized for TLS communications and software installation are expected to be stored on device. Code signing public keys/certificates are stored in the primary bootloader and programmed only by way of a validated image. Certificates used for TLS connections shall be stored in a read-only memory location.

Unless otherwise noted, all certificates used shall be derived from a Ford root CA.

## Keys, Certs, and Uses

Due to the inherently complex nature of a highly connected ECU, there are many keys and certificates needed to support secure features and communications.

### Cloud/SDN Connectivity

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| KeyID | AP | CP | Type | Usage | Delivery Method | Secret |
| KEY\_AP\_SYNCP\_0 | 🗹 |  | AES-128 | Device Master Key(AP)  For rekeying the application processor | Device Manufacture | Yes |
| KEY\_AP\_SYNCP\_[1-7] | 🗹 |  | AES-128 | Message Enc/Sign(AP)  Allows signing and encryption in addition to TLS | Device Manufacture  (Or using Key Rotation) | Yes |
| kPub\_FCL\_TLS\_CA | 🗹 |  | TLS Cert  (RSA-2048) | TLS Authentication | Device Provisioning | No |
| KEY\_CLOUD\_PSK | 🗹 |  | AES-128 | Device Provisioning PW | Device Manufacture | Yes |
| KEY\_CP\_SYNCP\_0 |  | 🗹 | AES-128 | Device Master Key(CP)  For rekeying the CAN processor | Device Manufacture | Yes |
| KEY\_AP\_SYNCP\_[1-7] |  | 🗹 | AES-128 | Message Enc/Sign(CP)  Allows signing and encryption in addition to TLS | Device Manufacture  (Or using Key Rotation) | Yes |

### ECU Diagnostics

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| KeyID | AP | CP | Type | Usage | Delivery Method | Secret |
| Kpub\_tokens | 🗹 | 🗹 | RSA-2048 Public Cert | Unlocks ECU diagnostics over serial connection (JTAG or UART) | Device Manufacture | Yes |
| Kdiag\_CAN |  | 🗹 | Diagnostic Password | Enable CAN DID Write | Device Manufacture | Yes |
|  |  |  |  |  |  |  |

### Software Installation

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| KeyID | AP | CP | Type | Usage | Delivery Method | Secret |
| Kpub\_cp\_sw |  | 🗹 | RSA-2048 Public Cert | Bootloader public cert for OTA/CAN image verification | Device Manufacture | No |
| Kpub\_ap\_sw | 🗹 |  | RSA-2048 Public Cert | Public signing x.509 certificate used for software installation on applications processor | Device Manufacture | No |

## Additional Details

In addition to the keys and certificates use inside the ECU, other expected values should be stored for response over CAN, and shall be include in communications as part of the message header. See **S13a SyncP functional specification** for more details.

### ESN

ESN or Electronic Serial Number is a unique-per-module value that corresponds to an ECU family. It is generated and stored in the ECU as part of the device manufacturing process. It is typically an eight (8) character value that is used for SyncP communications and reports as a part of the CAN diagnostic commands.

ESN prefix generation (3 characters) shall be determined by Ford. The suffix is then generated by the supplier and inserted at device manufacture. This value shall be read-only and is not considered a secret as it is widely used by vehicle and cloud systems. More information can be found in the **A51 Supplier Feed Specification.**

### Processor ID

As part of the SyncP communications protocol, the individual processors (AP and CP) are values within the header that determines which MCU is the message target. For more information, see **S13a SyncP functional specification.**

### IMEI

If an ECU has its own cellular chip, it shall have an associated IMEI that is used by the cellular carrier as part of network authentication. This should follow the **3GPP TS 23.003** format for generation. This information shall be part of the Ford provisioning process in instances that do not allow for ESN as the login username.

### Key Rotation

In addition to secured key storage, devices may be expected to allow for key and certificate rotation. Although not outlined in this document, the **KEY\_CP\_SYNCP\_0** and **KEY\_AP\_SYNCP\_0** are to be considered “Master keys” for the purpose of key rotation and shall not be used for normal messaging functions.

Please refer to the **Key Rotation and Rekeying Security Specification.**