



Secure CAN Logger

Duy Van
Advisor: Dr. Jeremy Daily



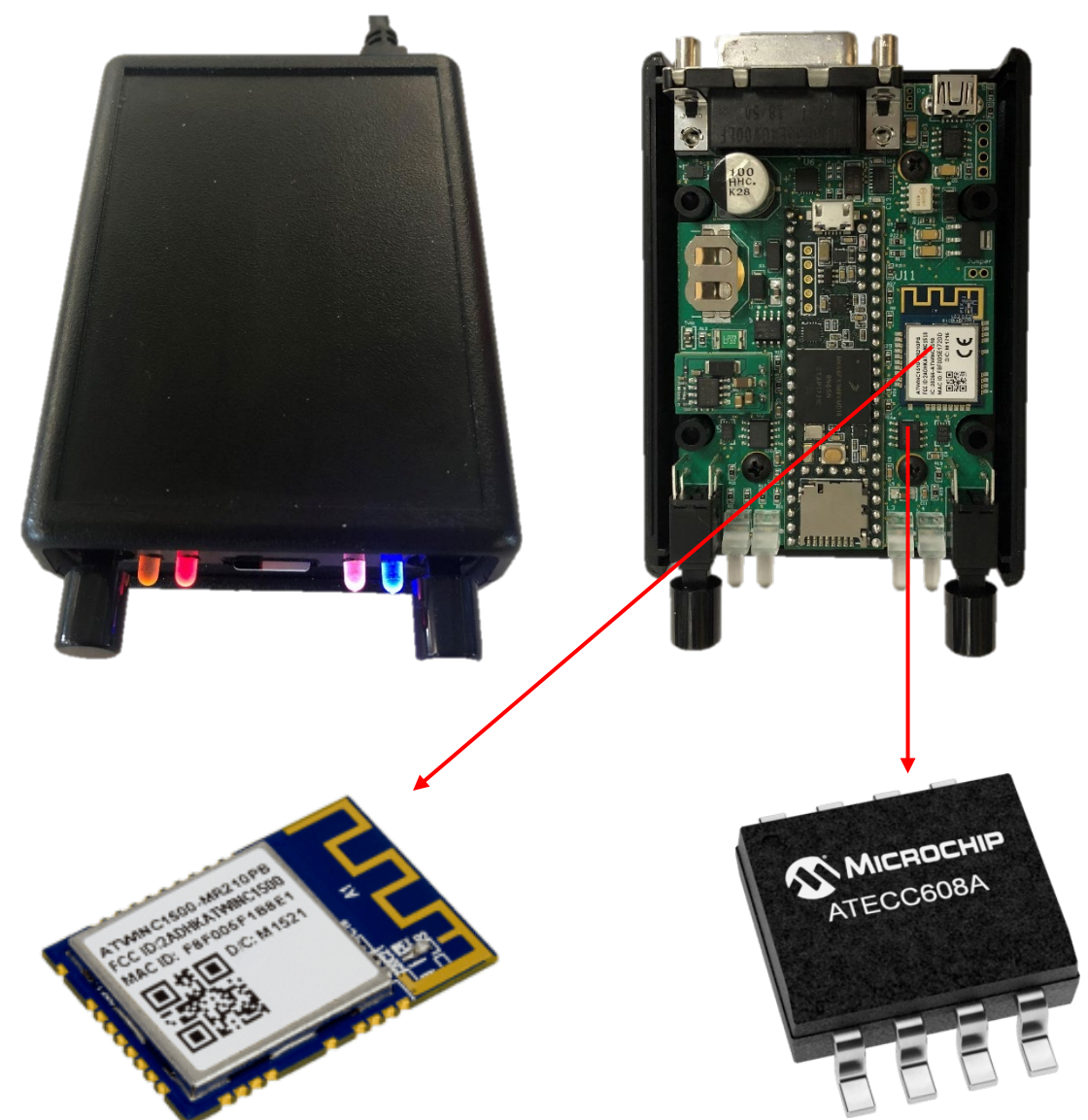
Motivation

- Heavy vehicle in-vehicle network communication network unknown.
- A large database of actual CAN logs is necessary for reference, verification, and validating cybersecurity strategies.
- Automatic processes are needed to scale the data collection efforts.
- When logging CAN data:
 - Data should be securely logged to ensure confidentiality and integrity.
 - Log files should be securely stored on cloud servers.
 - An API is necessary for uploading and downloading secured CAN data.
 - Data ownership and privilege is tightly controlled.

Hardware

CAN Logger 3

<https://github.com/SystemsCyber/CAN-Logger-3>

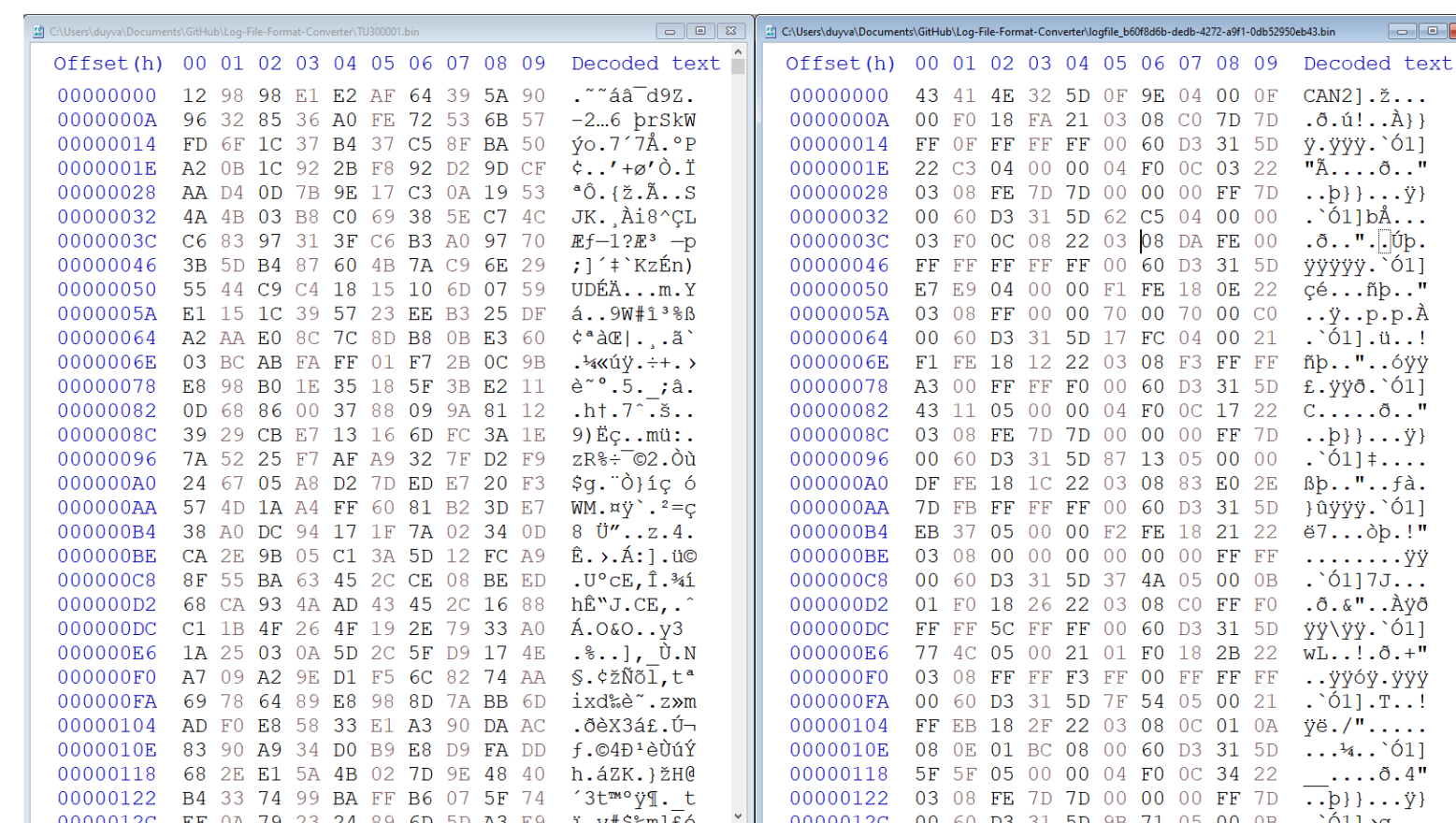


ATWINC1500
WiFi Chip

ATECC608A
Crypto Chip

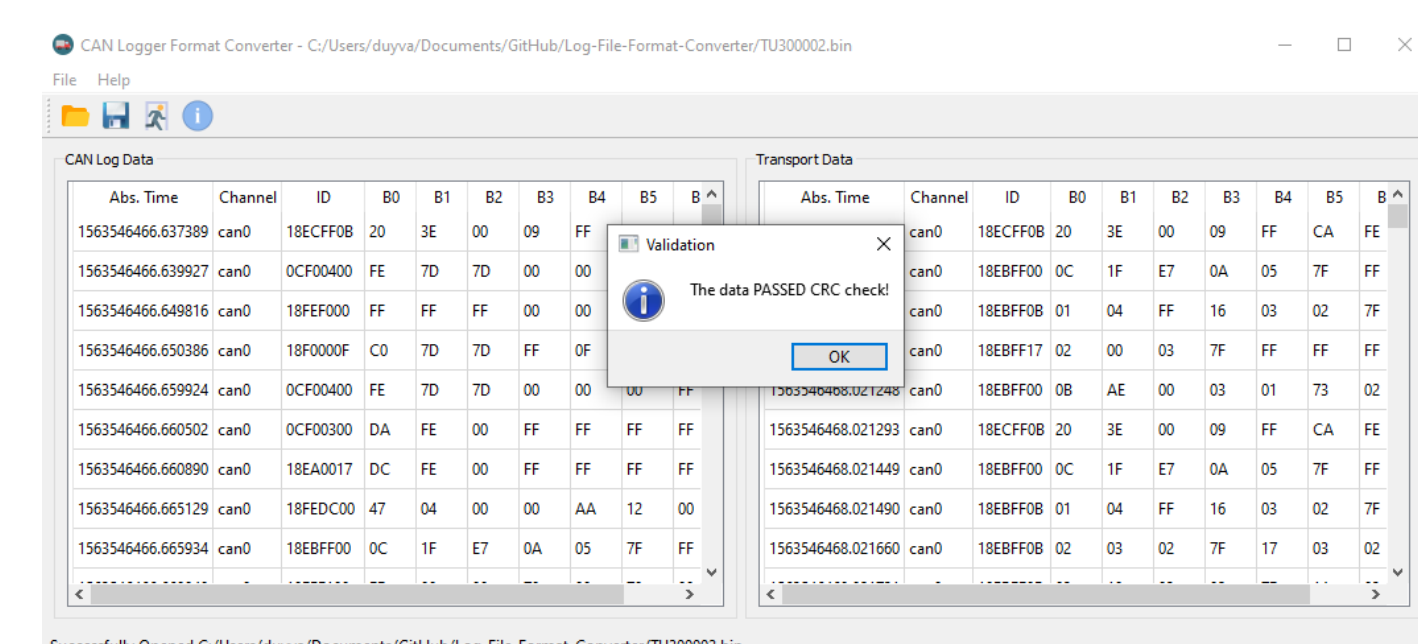
Features:

- Improved design from CAN Logger 2*
- Lower manufacturing cost
- MCP2517FD CAN Controller
- 2 push buttons, 4 LEDs
- ATWINC1500 WiFi Chip with physical Enable/Disable option
- MicroSD card slot for storage
- ATECC608A CryptoAuthentication
 - Secure key storage
 - ECDSA, ECDH – NIST Standard
- Crypto Acceleration Unit (CAU) built-in on Teensy 3.6 Freescale K66 Processor
 - AES encrypt and log data
 - Full BUS load test – 6.4Mbyte/sec
- CRC error checking
- CAN Error frame logging capability



Encrypted Log

Unencrypted Log



Converting Log File to J1939 with CRC Error Checking

Implementation

Key Exchange Provisioning:

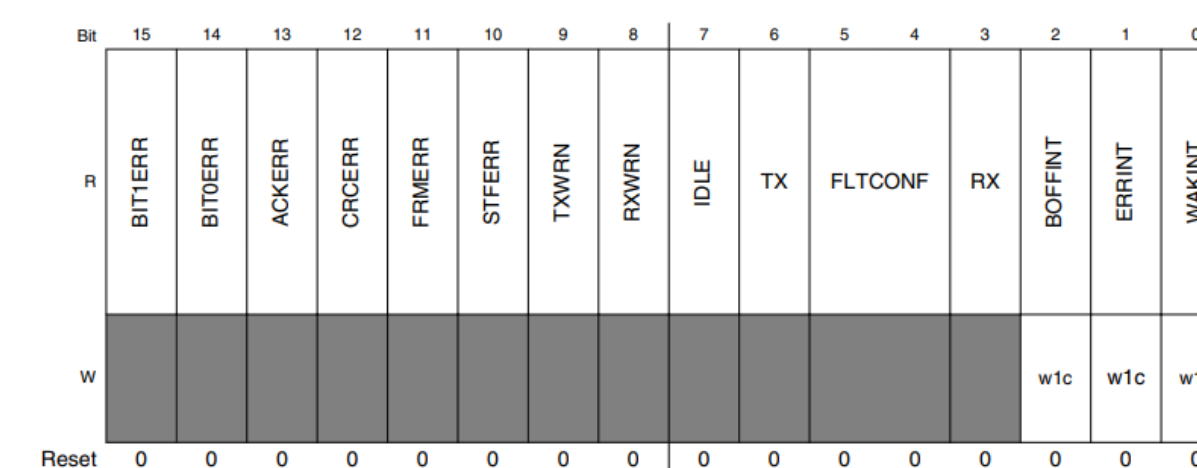
- Exchange public key in the one-time provisioning process.
- Keys are securely stored in the logger hardware security module and on the server.
- Shared secret key is made from Elliptic-Curve Diffie-Hillman (ECDH) for logging session.

Logging:

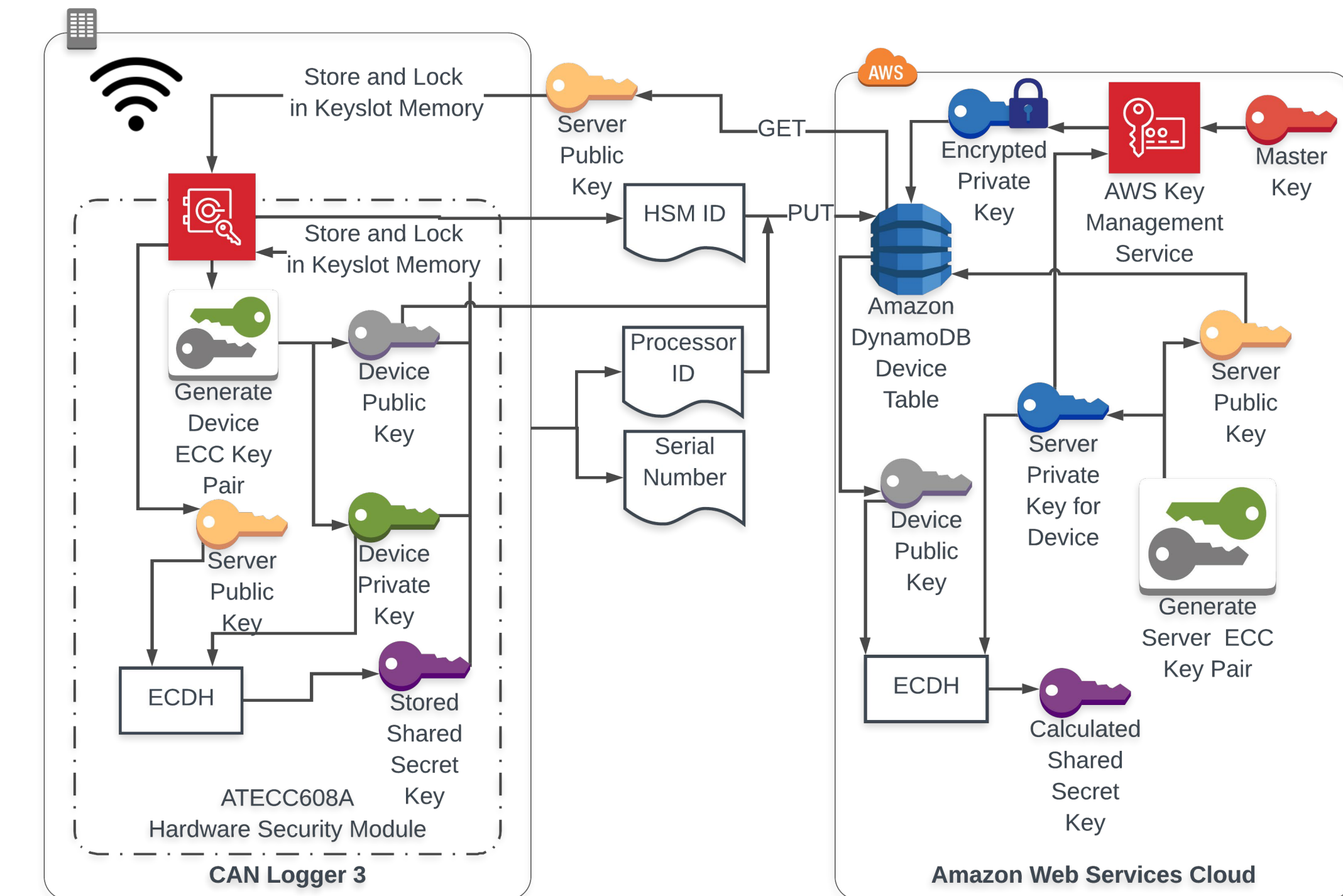
- Device generates an AES session key to encrypt log file
- Device envelope encrypts AES session key using the shared secret key.
- Device signs the encrypted log.
- Server computes shared secret key, which is used to decrypt log file
- Server verifies log file integrity

Data Analysis:

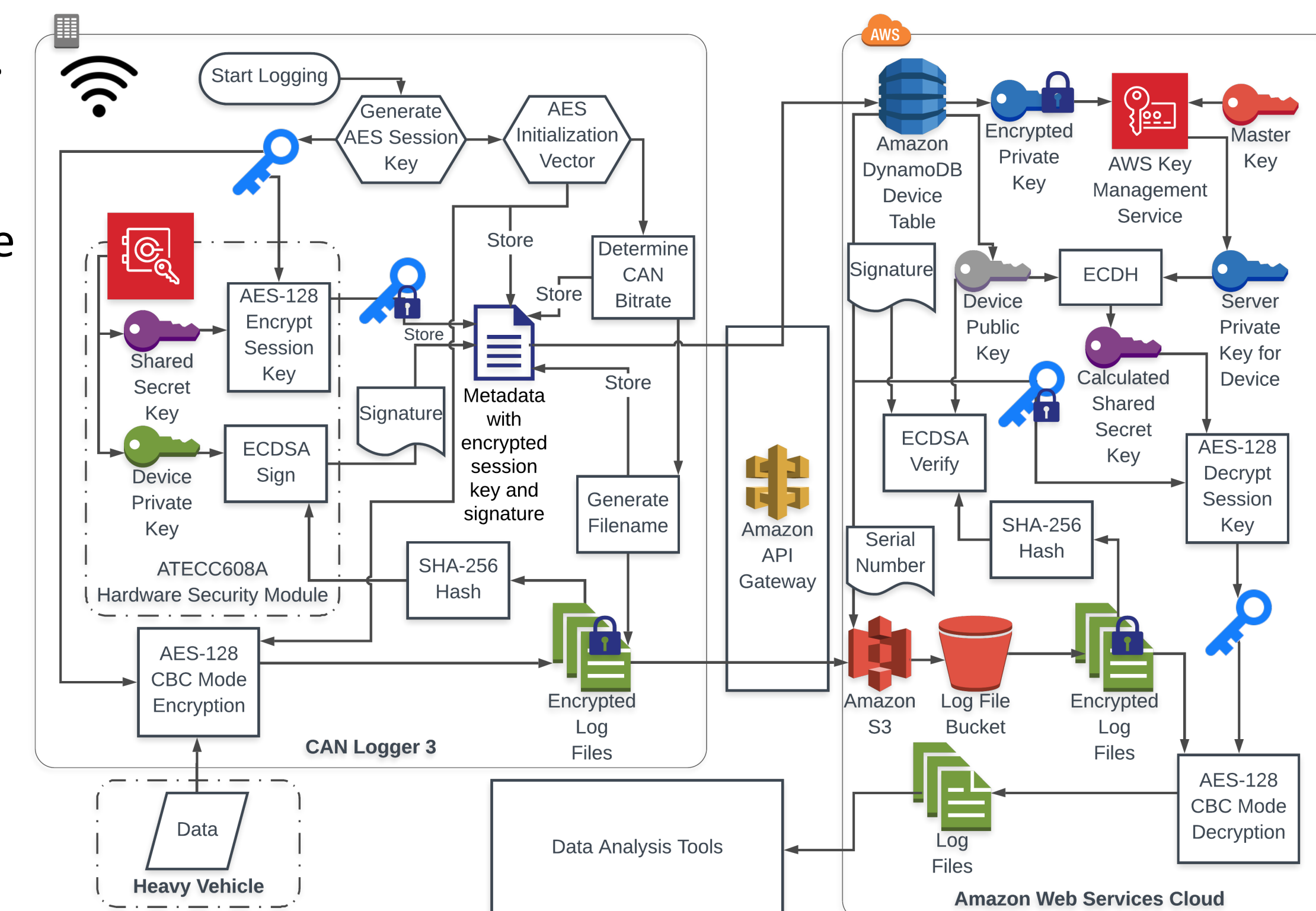
- Convert and decode
 - Time stamp, ID, Data
 - Error frame presence
 - Plot parameters



CAN Error Register for
Teensy 3.6 Processor – K66



Key Exchange Provision Diagram



Logging Process Diagram

*<https://github.com/Heavy-Vehicle-Networking-At-U-Tulsa/CAN-Logger-2>