Securing Cloud Communication on Embedded Devices
Ram Rohit Gannavarapu
Advisor: Dr. Jeremy Daily

Purposes:
• Securing the Cloud communication for modern day smart vehicles.
• Secure private key storage on hardware.

Hardware:
• Microprocessor: Mini-SSS3 powered with Teensy 4.0
• Hardware Security Module: Microchip ATECC608B Crypto Auth Platform

Software:
• PlatformIO
• Arduino and Teensyduino
• ArduinoBearSSL
• ArduinoECCX08
• Amazon Web Services Console

Procedures:
• Generate a certificate signing request (CSR) with the private key stored on the ATECC608 chip to get a certificate signed by registering it with the cloud provider.
• Provision the device with certificate issued by the cloud provider.

Generating Certificate Signing Request
• Once the ATECC608B is configured with a private key and locked the private key can not be accessed again by the host system.
• All the related functions which require private key are only accessible to the ATECC chip and output of those functions are relayed back to the host MCU.

Storing a compressed certificate in ATECC608
• X.509 certificates are larger than what will fit into a single ATECC608B-TNGTLS device slot, hence, a compressed format is used to store the certificate.

Utilizing Preconfigured ATECC608-TNGTLS
• The Microchip ATECC608B-TNGTLS is a pre-provisioned variant of the ATECC608B.
• The device comes pre-configured and pre-provisioned with default thumbprint certificates which can be used to make a connection to AWS IOT, Azure and Google Cloud Services.

Secure communications based on pre-provisioned certificate.