Application Using Secure Element and TrustZone on SAML11

This application demonstrates a security use case on SAML11 by combining TrustZone technology and secure element ATECC508.

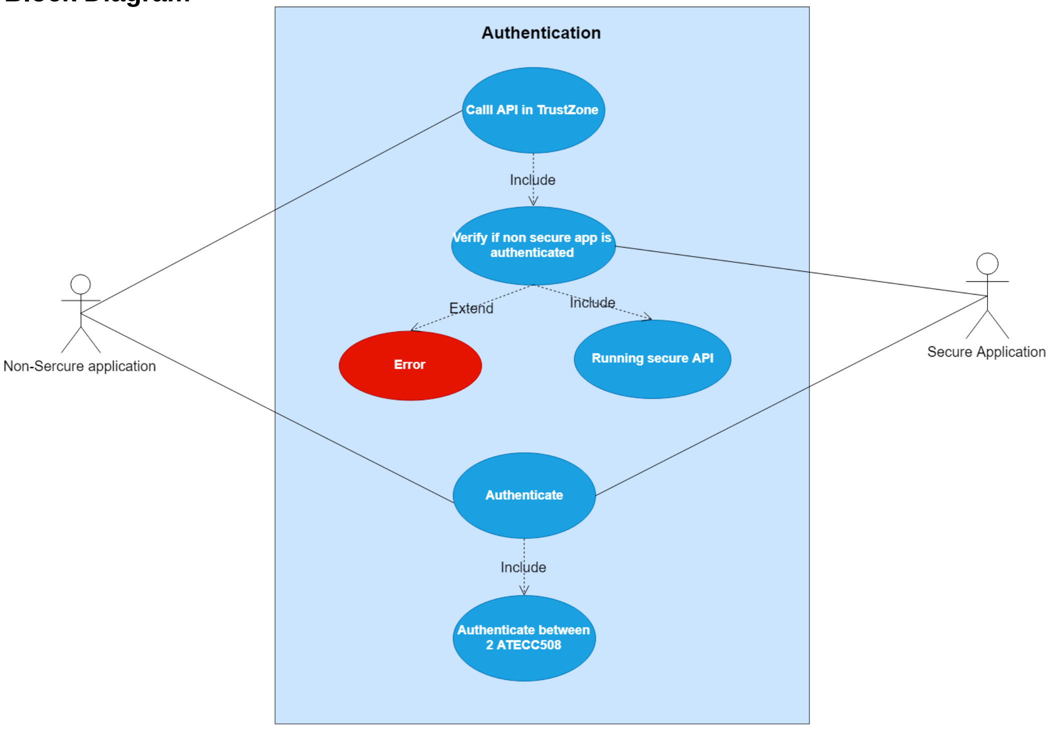
For more information please visit:

Github link

TrustZone
TrustZone provides the flexibility for hardware isolation of memories and peripherals, therefore reinforcing the ability of Intellectual Properties (IP) and Data protection. SAML11 provides up to six regions for the Flash, up to two regions for Data Flash, up to two regions for SRAM and the ability to assign peripherals, I/O pins, interrupts to secure or non-secure application.

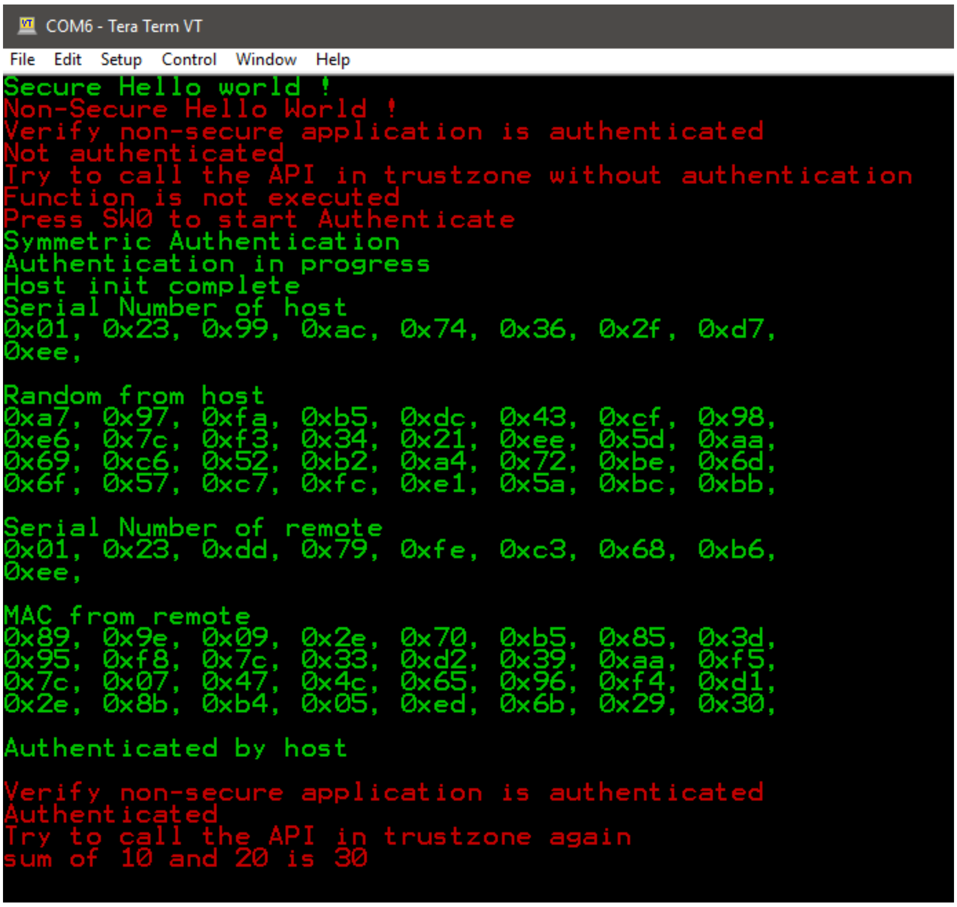
ATECC508
The Microchip ATECC508A integrates ECDH (Elliptic Curve Diffie Hellman) security protocol an ultra-secure method to provide key agreement for encryption/decryption, along with ECDSA (Elliptic Curve Digital Signature Algorithm) sign-verify authentication for the Internet of Things (IoT) market including home automation, industrial networking, accessory and consumable authentication, medical, mobile and more.

Block Diagram



Description

Inside SAML11, there are two application running, which are the secure and non-secure application. When the non-secure application tries to call the API in TrustZone area, the secure application checks if the non-secure one is already authenticated and allows the API to run or showing error message.



```
Secure Hello world !
Non-Secure Hello World !
Verify non-secure application is authenticated
Not authenticated
Try to call the API in trustzone without authentication
Function is not executed
Press SW0 to start Authenticate
Symmetric Authentication
Authentication in progress
Host init complete
Serial Number of host
0x01, 0x23, 0x99, 0xac, 0x74, 0x36, 0x2f, 0xd7,
0xee,

Random from host
0xa7, 0x97, 0xfa, 0xb5, 0xdc, 0x43, 0xcf, 0x98,
0xe6, 0x7c, 0xf3, 0x34, 0x21, 0xee, 0x5d, 0xaa,
0x69, 0xc6, 0x52, 0xb2, 0xa4, 0x72, 0xbe, 0x6d,
0x6f, 0x57, 0xc7, 0xfc, 0xe1, 0x5a, 0xbc, 0xbb,

Serial Number of remote
0x01, 0x23, 0xdd, 0x79, 0xfe, 0xc3, 0x68, 0xb6,
0xee,

MAC from remote
0x89, 0x9e, 0x09, 0x2e, 0x70, 0xb5, 0x85, 0x3d,
0x95, 0xf8, 0x7c, 0x33, 0xd2, 0x39, 0xaa, 0xf5,
0x7c, 0x07, 0x47, 0x4c, 0x65, 0x96, 0xf4, 0xd1,
0x2e, 0x8b, 0xb4, 0x05, 0xed, 0x6b, 0x29, 0x30,

Authenticated by host

Verify non-secure application is authenticated
Authenticated
Try to call the API in trustzone again
sum of 10 and 20 is 30
```

The non-secure application is initialized by the secure application. The non-secure application can access to the API by first authenticating to the secure application. The secure application carries out the authentication process and return the status. If the authentication is successful, the non-secure application is allowed to access the API.

Possible Application

- IP protection
- Authentication
- Anti-counterfeit

Features/Benefits

- IP protection
- Software isolation
- Authentication
- Cryptography

Key Components

- SAML11
- Arm TrustZone
- ATECC508