ECC608A Primer

Golden Bits Software
Microchip Security Design Partner
Dean Gereaux

goldenbits.com

Overview

Dedicated IC design to store keys and perform crypto operations

- Key storage. Secure, hardware tamper proof hardware
- Mini HSM (Hardware Security Module)
- 16 slots to store keys, generate keys, store data.
- Elliptical Curve Crypto operations. Signing, key generation, signature validation. ECC 256 bit Prime Curve only.
- ECC608A is latest version of crypto auth chip family. Previous versions ECC508A, ECC204.

Value

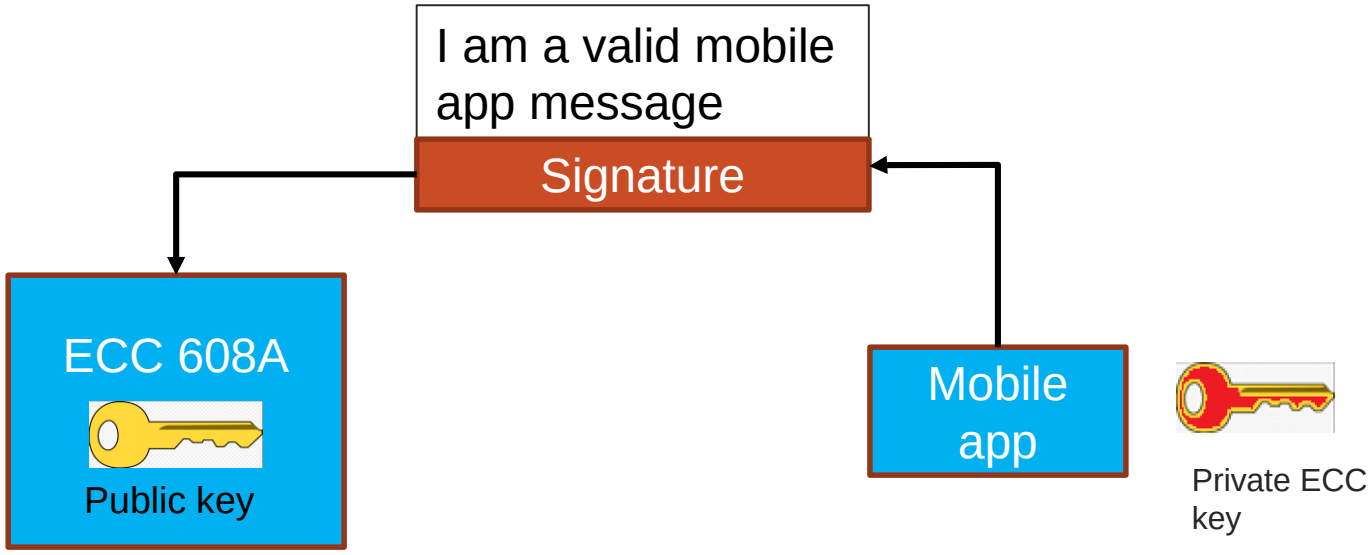
What does a dedicated ECC608A do for my design?

- Securing your product is no longer optional.
  - Customer expect secure products, reduce risk, industry compliance.
- Securing user information.
- Ability to authenticate device, prevent rouge access.
- Crypto keys used to encrypt data, securely store in ECC608A.

Use Case

ECC, Asymmetric key validation

- Authentication. Core functionality.
- Sub parts of Authentication are key storage and ECC crypto ops.

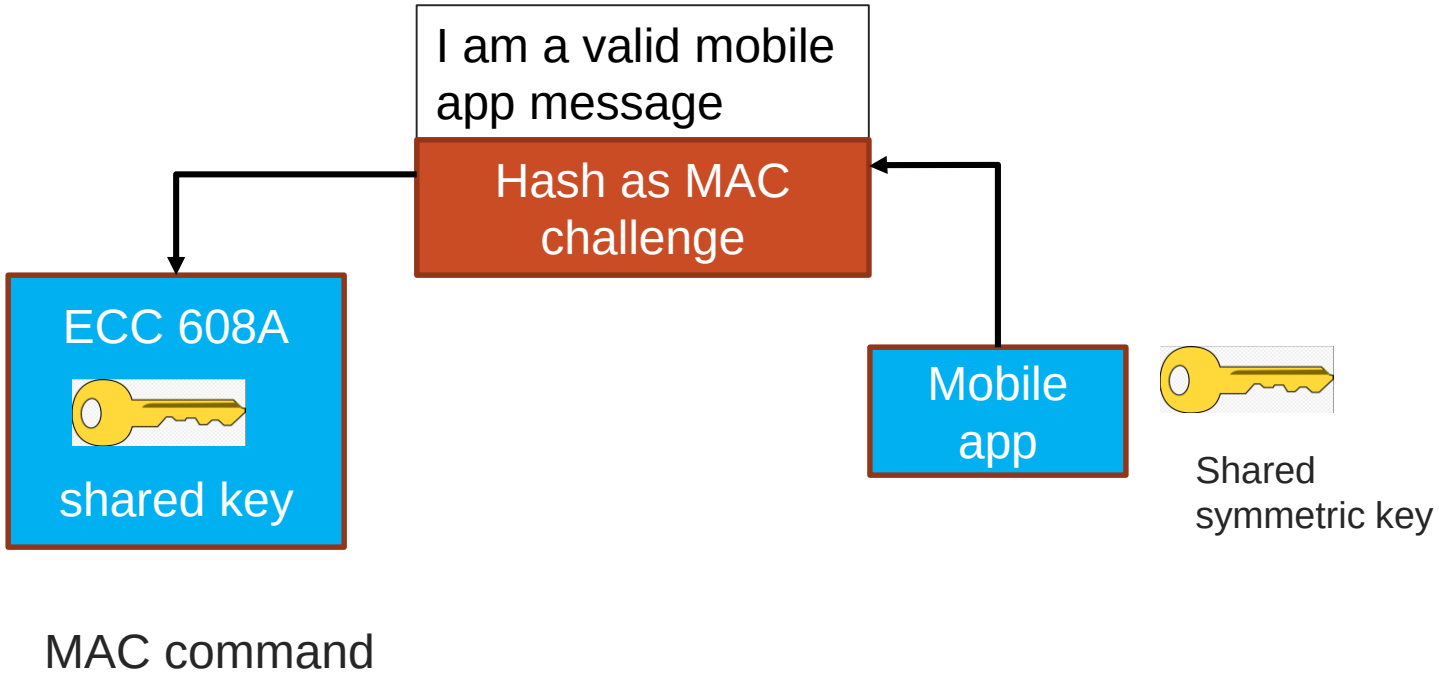


Public key stored in slot, known good key

Use Case

MAC Validation with Shared key

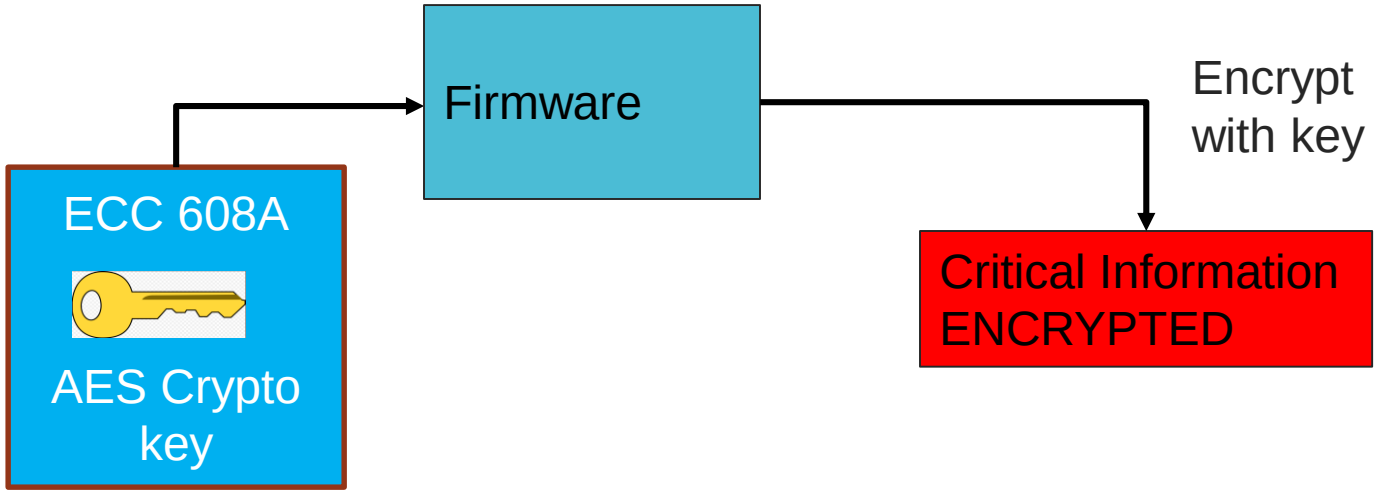
- Use of shared 32 byte symmetric key.
- Create hash of message, use as part of MAC challenge.
- MAC verified using pre-shared key.



Use Case

Storing keys

- Securely store encryption key in ECC608A.
- Key not exposed in firmware itself.
- Use to encrypt critical data such operational parameters or user information.



Configuring ECC608A

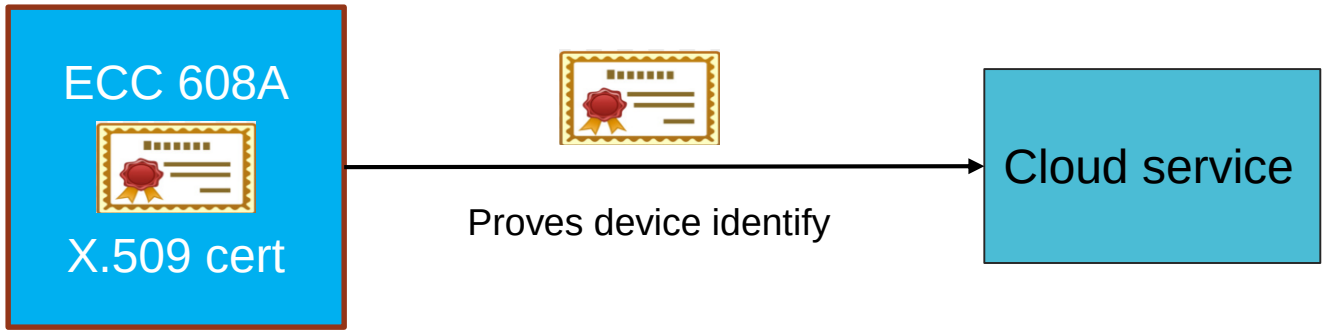
Flexible configuration

- 16 key slots.
- Each Slot can be configured as a key or data.
- Configure slot as read only, writeable, or containing ECC key and more.
- Configure during manufacturing or first boot.
- After configuring, ECC608A is locked down and can not be changed.
- During first configuration, can generate unique ECC keypair for device, a unique id for each device.

Certificates

X.509 Certificates

- Can create a unique device certificate for each device.
- Very important feature.
- A small, low power, constrained device can have a digital certificate!!! Just like larger server based systems.
- Excellent solution for IoT devices.



CryptoAuth lib

Software support

- C Library provided by Microchip to interface with ECC608A.
- Code avail on Git: https://github.com/MicrochipTech/cryptoauthlib
- HAL Layer, specific to platform. Lots of HAL interfaces provided.

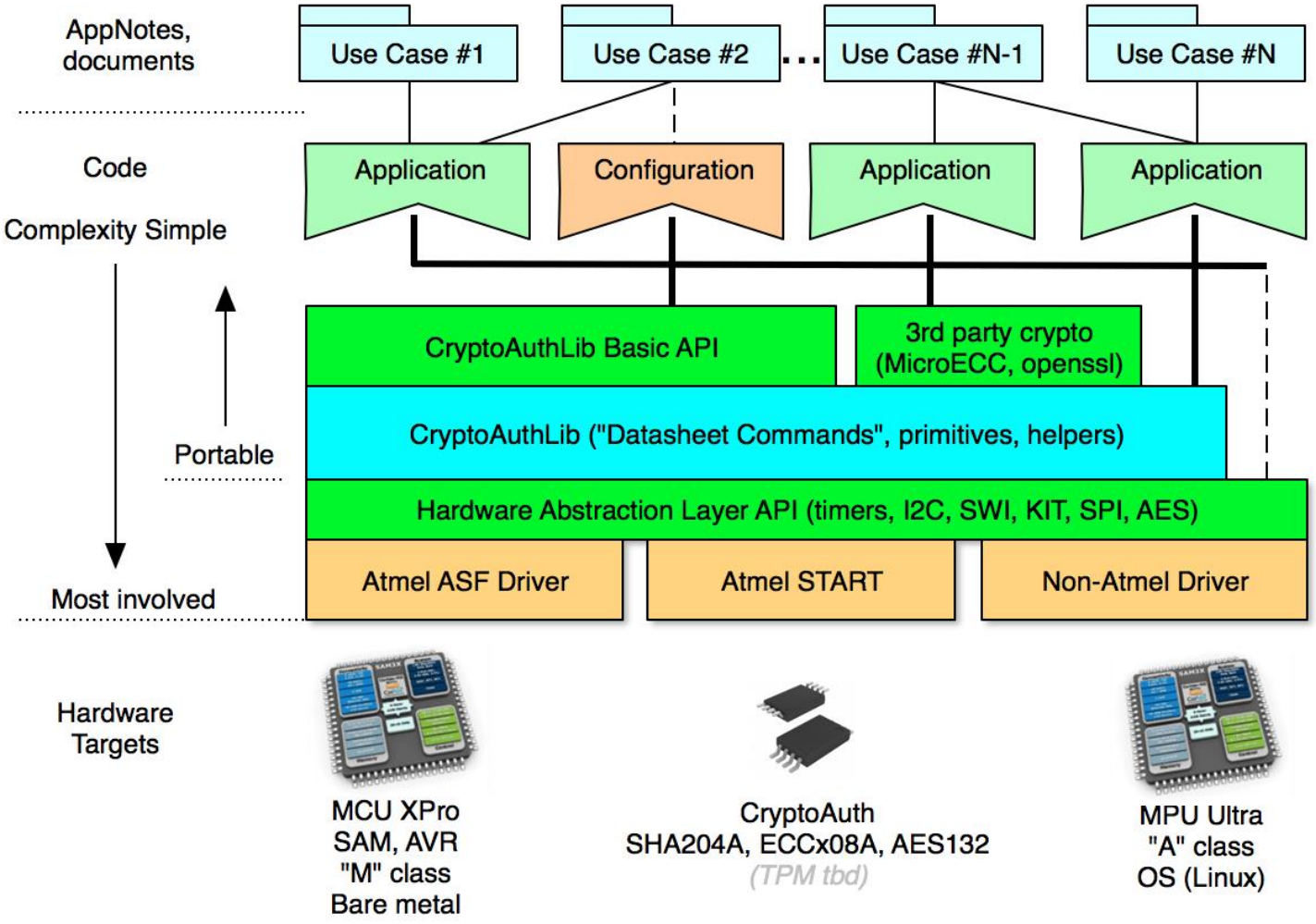
HAL interface, function pointers

```
struct atca_iface
{
    ATCAIfaceType mType;
    ATCAIfaceCfg *mIfaceCFG;    // points to previous defined/given Cfg object, caller manages this

    ATCA_STATUS (*atinit)(void *hal, ATCAIfaceCfg *);
    ATCA_STATUS (*atpostinit)(ATCAIface hal);
    ATCA_STATUS (*atsend)(ATCAIface hal, uint8_t *txdata, int txlength);
    ATCA_STATUS (*atreceive)(ATCAIface hal, uint8_t *rxdata, uint16_t *rxlength);
    ATCA_STATUS (*atwake)(ATCAIface hal);
    ATCA_STATUS (*atidle)(ATCAIface hal);
    ATCA_STATUS (*atsleep)(ATCAIface hal);

    // treat as private
    void *hal_data;     // generic pointer used by HAL to point to architecture specific structure
};
```

CryptoAuth lib

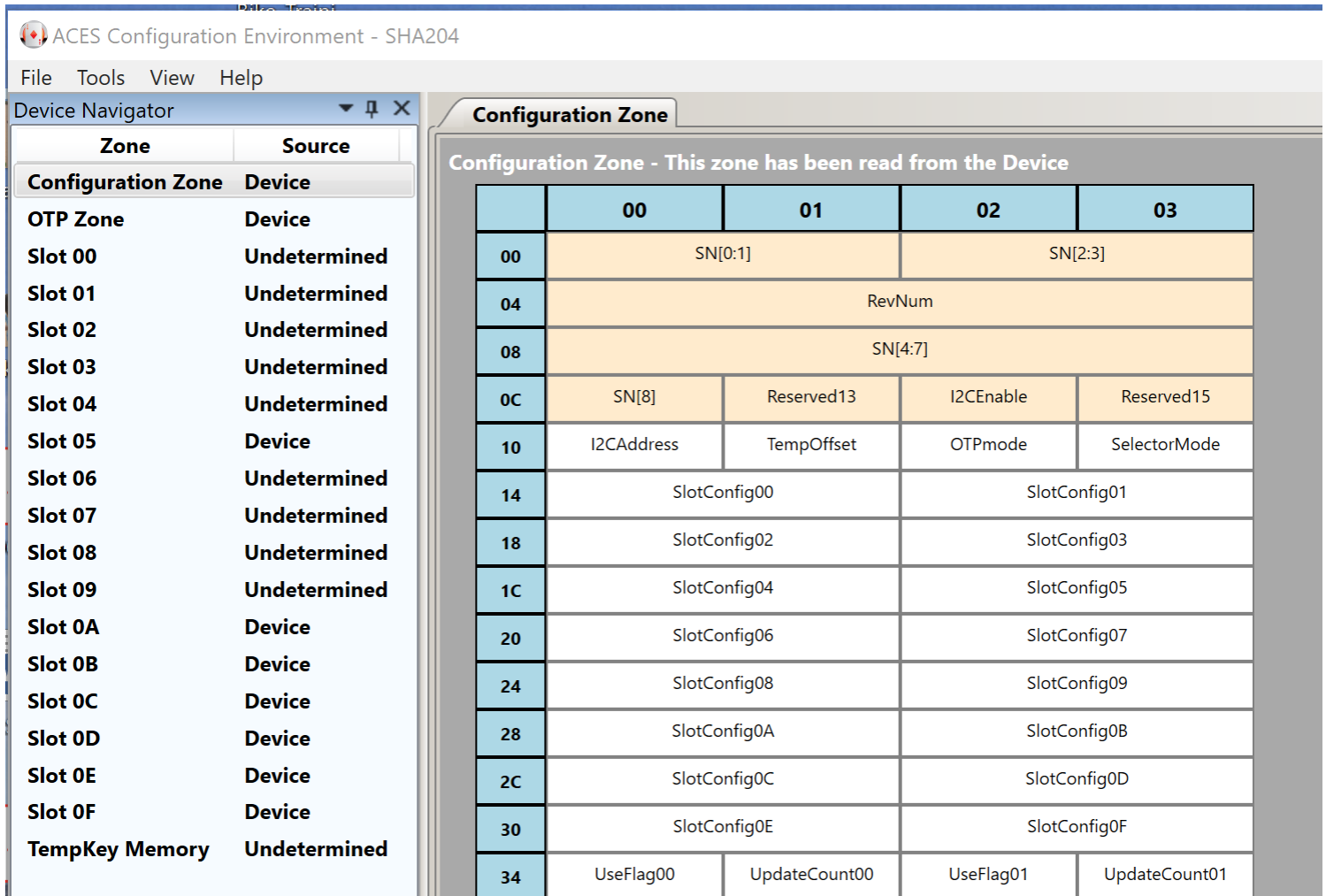


CryptoAuth lib

- Review documents in subdirectory: **`cryptoauthlib/docs`**

ACES Tool

Helpful tool to configure device.



ACES Tool

Sending commands.

- Example of sending commands to ECC608A.
- Command window, can see exact bytes sent.
- Great place to start experimenting with ECC608A.

```
07 00 00 00 02 80 38
Random Command Sent:
07 1B 00 00 00 24 CD
RandomCommand Received:
23 93 AD 91 FC 36 4D 1A CE AC 76 ED F9 9D B4 9E FA B8 7B AB 0E B1 3E 37 F0 DA 1B 98 BF 12 E3 78 CD B1 B3
```

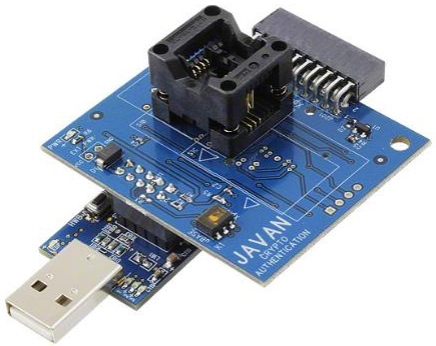
- Random command ‘1B’, Param 1 ‘0’, Param 2 ‘00’
- Response, ‘23h’ number of response bytes.
- ‘B1 B3’ checksum.

USB Device

Development tools

- Easy to goof up configuration.
- SOIC slot, can simply pop in another blank device.
- Great for development purposes.

AT88CK101SK-SSH-XPRO



https://www.digikey.com/product-detail/en/microchip-technology/AT88CK101SK-SSH-XPRO/AT88CK101SK-SSH-XPRO-ND/4496853

Takeaways

Important stuff to remember

- Securing your product is no longer optional
- ECC608A low cost device - flexible, secure
- Great solution for constrained devices.
- You can create device X.509 certificates!!
- Solid tools and software from Microchip