APPLICATION NOTE

Atmel CryptoAuthentication Data Zone CRC Calculation

ATSHA204A, ATECC108A, and ATECC508A

Introduction

In the process of personalizing the Atmel® CryptoAuthentication™ ATSHA204A, ATECC108A, and ATECC508A crypto element devices, it is necessary to lock the configuration, OTP and Data Zones before deploying. Calculating the CRC for the Data and OTP Zone Lock command can be tricky depending upon the key and slot configurations.

The CRC formula itself is the same as used for all other interactions with these crypto devices. Choosing the content that goes into the CRC requires close attention.

This Application Note discusses how the Data and OTP Zone CRC calculation is performed.

1 Solution Overview

The crypto device Data zone is locked by the host that is doing the provisioning by concatenating the contents of the Data zone and OTP zone, computing the CRC on that content and issuing the Lock command with a mode of one and the computed CRC. If the CRC passed to the `Lock` command matches the crypto devices internal CRC calculation, the Data Zone is locked; otherwise, an error is returned indicating a problem with the provisioning process.

The concatenated content is intuitively sequential from Slot 0 through Slot F, and followed by the OTP zone.

In general, all bytes of the OTP Zone and all bytes of the Data Zone are candidates for inclusion in the CRC computation. However, in practice, some parts of the Data Zone may not be included based upon the key configuration for that slot. Also, depending upon the slot configuration and how the slot contents were populated there can be some dynamic elements, so the specific contents can change slightly based upon the state of the device when the Data Zone `Lock` command is issued.

PREREQUISITES:

This Application Note assumes knowledge on how to construct commands and send them to the crypto device, and how to read responses from the device. The user therefore must have access to the code to communicate with the crypto device.

Please refer to the ***CryptoAuthentication ATECC108A/508A Development Library*** for C programming language at:
http://www.atmel.com/tools/CryptoAuthentication_ATECCx08A_Development_Library.aspx

Reference the respective ATSHA204A, ATECC108A, or ATECC508A full datasheet (available under NDA) while working through this solution.

1.1 Slots with ECC Private Keys

Slots in the Data Zone that contain ECC private keys are never included in the CRC computation for the Data Zone.

Specifically, a slot that will be skipped in the calculation has its KeyConfig Bit 0 set to 1 (KeyConfig:0 == 1). Refer to the table which defines KeyConfig bits per slot in the ATSHA204A or ATECCx08A full datasheet.

Note that the amount of the data included in the CRC computation could be less than the size of the total Data Zone.

1.1.1 Internally Generated Private Keys

ECC Private keys which are created within the crypto device via the `KeyGen` command are never readable under any circumstances. Consequently, there is no way for a host to know the private key in order to make the Data Zone CRC computation. Therefore, it is not included in the CRC data since the host cannot generate the CRC for the contents of the Data Zone without knowing the private key.

1.1.2 PrivWrite Private Keys

If a private key is written into the device using a `PrivWrite` command as opposed to being generated internally by `KeyGen`, then the host does know the private key. Even in this case, the private key is not included in the Data Zone CRC computation.

1.2 Dynamically Changing Data Zone

If a slot contains an ECC public key that needs to be validated, then the contents of the slot are modified to include a flag that indicates the validation state. That flag is stored in the upper nibble of the first byte of the slot and its current value must be taken into account when calculating the Data Zone CRC. This validation flag needs to be considered under the following conditions:

- The slot is 8 through F.
- The KeyConfig Private bit is zero (KeyConfig:0) and the KeyConfig PubInfo bit is one (KeyConfig:1).
- The KeyConfig KeyType is not 7 (KeyConfig:2-4).

If a slot meets the above requirements, the upper nibble of the first byte could be one of three values:

- `0xF` – If the slot was never written to. This is the default value.
- `0xA` – If any portion of the slot was written to, but one hasn't validated it yet with the Verify command.
- `0x5` – If the slot was successfully validated using the Verify command.

Please refer to the table that provides details on the Private and PubInfo bits of KeyConfig in the ATSHA204A or ATECCx08A full datasheet.

2 CRC Calculation Code

The code below calculates a CRC that is compatible with all the commands of the ATSHA204A or ATECCx08A crypto device.

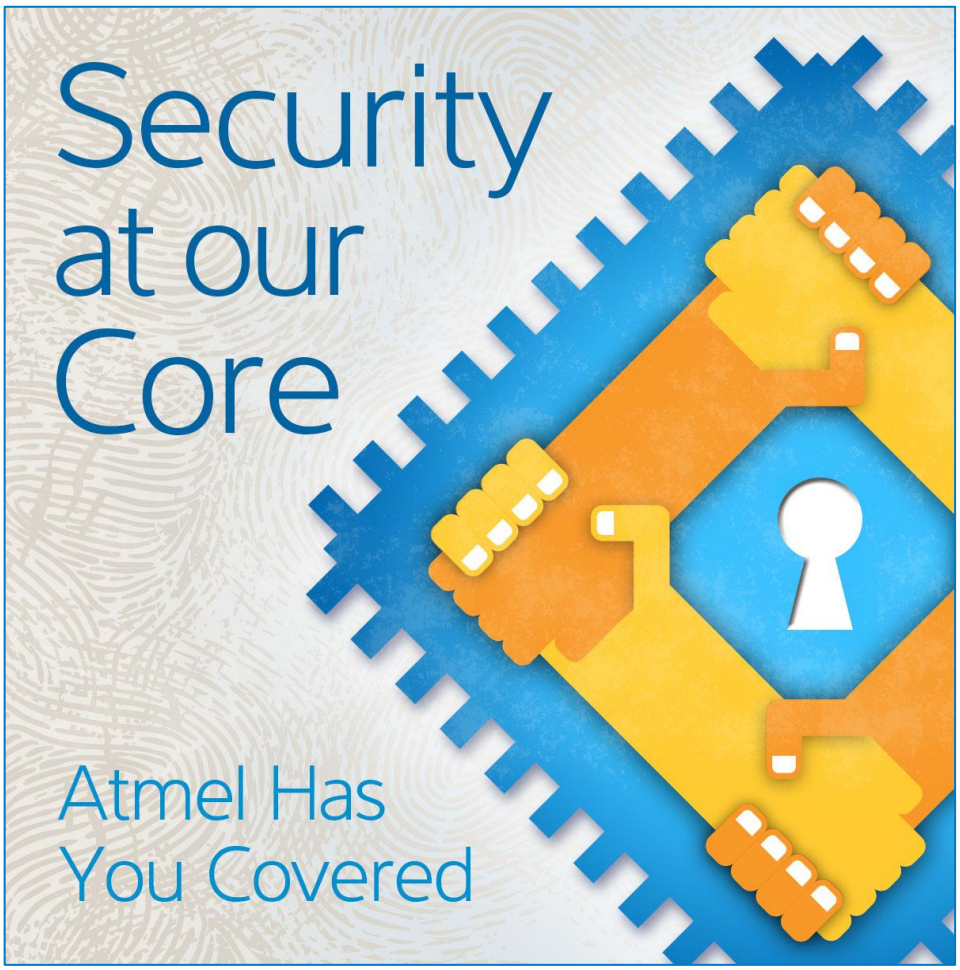
CRC Calculation Code

```
/** \brief This function calculates CRC.
*
* \param[in] length number of bytes in buffer
* \param[in] data pointer to data for which CRC should be calculated
* \param[out] crc pointer to 16-bit CRC
*/
void atca_calculate_crc(uint8_t length, uint8_t *data, uint8_t *crc) {
    uint8_t counter;
    uint16_t crc_register = 0;
    uint16_t polynom = 0x8005;
    uint8_t shift_register;
    uint8_t data_bit, crc_bit;

    for (counter = 0; counter < length; counter++) {
        for (shift_register = 0x01; shift_register > 0x00; shift_register <<= 1) {
            data_bit = (data[counter] & shift_register) ? 1 : 0;
            crc_bit = crc_register >> 15;
            crc_register <<= 1;
            if (data_bit != crc_bit)
                crc_register ^= polynom;
        }
    }
    crc[0] = (uint8_t) (crc_register & 0x00FF);
    crc[1] = (uint8_t) (crc_register >> 8);
}
```

3 Revision History

Doc Rev.	Date	Comments
8908A	08/2015	Initial document release.



Atmel | Enabling Unlimited Possibilities®

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**