APPLICATION NOTE

Generating Random Secrets

ATSHA204A, ATECC108A, and ATECC508A

Description

When defining a secret that will be used for cryptographic authentication, it is important that the secret is not predictable in any way. The classic way to do that is by using a high quality random number.

The Atmel® CryptoAuthentication™ devices can generate high-quality random numbers which can be deployed for any purpose, including as part of the crypto protocols of the device itself. Because each 256-bit random number is guaranteed to be unique from all numbers ever generated on this or any other device, its inclusion in the protocol calculation ensures that replay attacks (i.e. re-transmitting a previously successful transactions) always fail. This random number generator is very useful for authentication or for any other system purposes.

Topics

- Why a Truly Random Secret Matters
- What Makes a High-quality Secret
- How to use ACES (Atmel Crypto Evaluation Studio) software to access high-quality true random numbers for personalization of the crypto devices or for other external application software.

1 Random Secrets

For a secret to be truly random it must be unpredictable, non-correlated, and unrepeatable.

Why is true randomness important for secrets?

1. The strength of cryptographic security is mathematically linked to the randomness of the secrets used.
2. If a secret is not random, an exhaustive attack may become possible.

Generating a random number using a deterministic computer can be a challenge. Random number algorithms use a seed along with a predictable algorithm to generate a pseudo-random number. It is therefore the randomness of the seed that will determine the ultimate quality of the random number.

In the crypto devices, the random seed comes from variations at a quantum scale within the device. The inherent quantum mechanical entropy of the circuitry within the device provides a truly random seed for the `Random` and `Nonce` Commands.

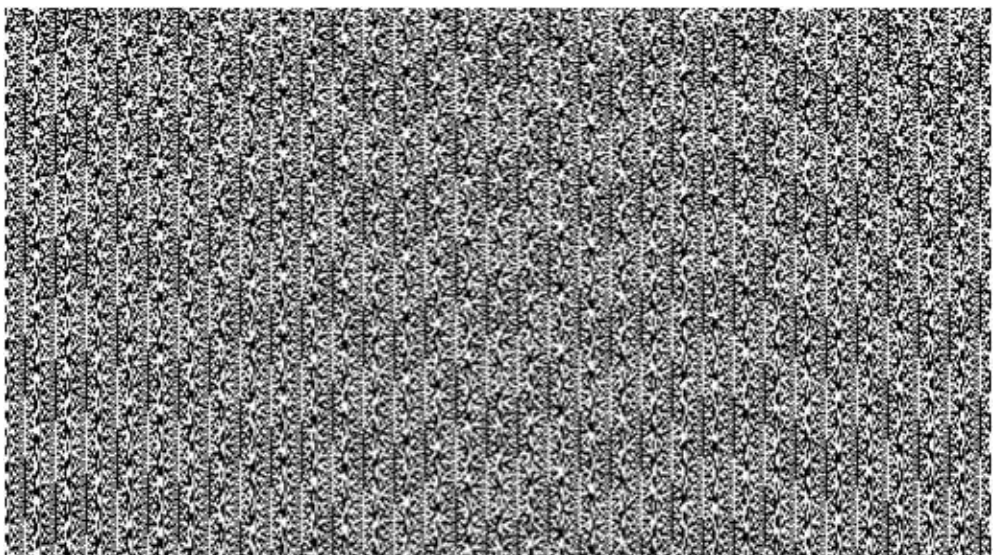
1.1 Less Secure Secrets

There are some techniques and practices that should be avoided. These practices can produce secrets with lower entropy and may be discoverable.

1.1.1 Using a Pseudo Random Number Generator

Most operating systems have a Pseudo Random Number Generator (PRNG) which is useful for workstation randomness. The problem with a PRNG is that it does not have a truly random seed to work with, and as a result patterns can emerge. See the visualization of the Windows PRNG below.

Figure 1-1. Windows PRNG



http://www.random.org/analysis/#visual

1.1.2 Making Up a Secret

Made up by a human secret will always have a pattern to it. The main problems noted below:

- People get bored so patterns will occur quickly.
- The human brain has a lot of structure devoted to pattern recognition and creation.
- Truly random numbers will contain repeats which humans try to avoid.
- Humans aren't good with large numbers.

2 Walkthrough

This section outlines the steps involved to access the crypto device's random function by using the ACES application software.

2.1 Device Configuration

Since keys will not be used, the only requirement is to have the device locked per the datasheet's instructions.

The Random Command section of the datasheet states:

"Prior to the configuration section being locked, the random number generator produces a value of 0xFF, 0xFF, 0x00, 0x00, 0xFF, 0xFF, 0x00, 0x00 to facilitate testing"

1. Launch ACES Configuration Environment (ACES CE) with a crypto device on an AT88CK590 or AT88CK101 kit for example.

Figure 2-1. AT88CK101 Development Kit

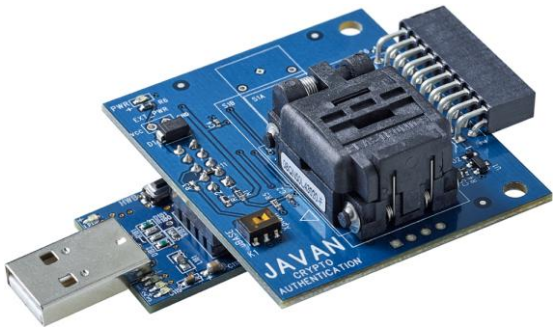


Figure 2-2. AT88CK590 Demo-evaluation Kit

2. Observe the locked state of the crypto device in the ***Lock State*** dialog box located in the lower left corner of the ACES application.

Figure 2-3. Lock State is Unlocked

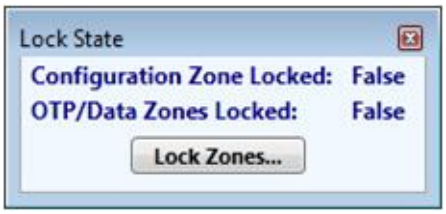
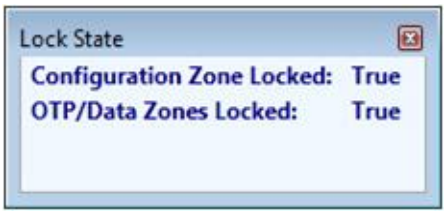
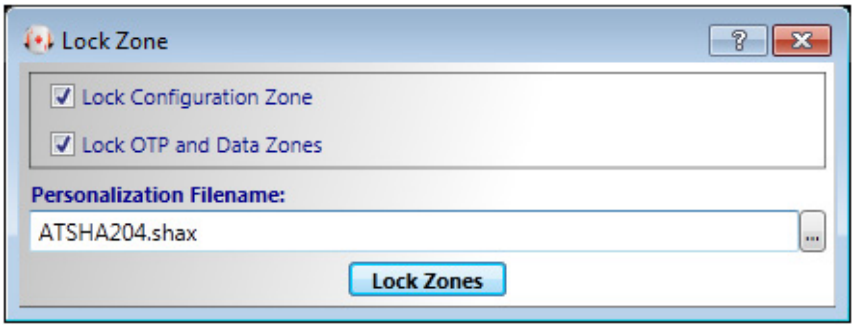


Figure 2-4. Lock State is Locked



3. If the lock state is locked, then skip to Section 2.2. "Random Secret Generation".
4. If the lock state is unlocked, then the crypto device device needs to be locked.
   - Select the ***Lock Zones*** button in the ***Lock State*** dialog box shown in Figure 2-3.
   - The ***Lock Zone*** dialog box will be displayed as shown in Figure 2-4.
   - Select the ***Lock Configuration Zone*** check box.
   - Select the ***Lock OTP and Data Zones*** check box.
   - Select the ***Lock Zones*** button.
   - The ***Lock Successful*** message will be displayed.

Figure 2-5. Lock Zone Dialog Box



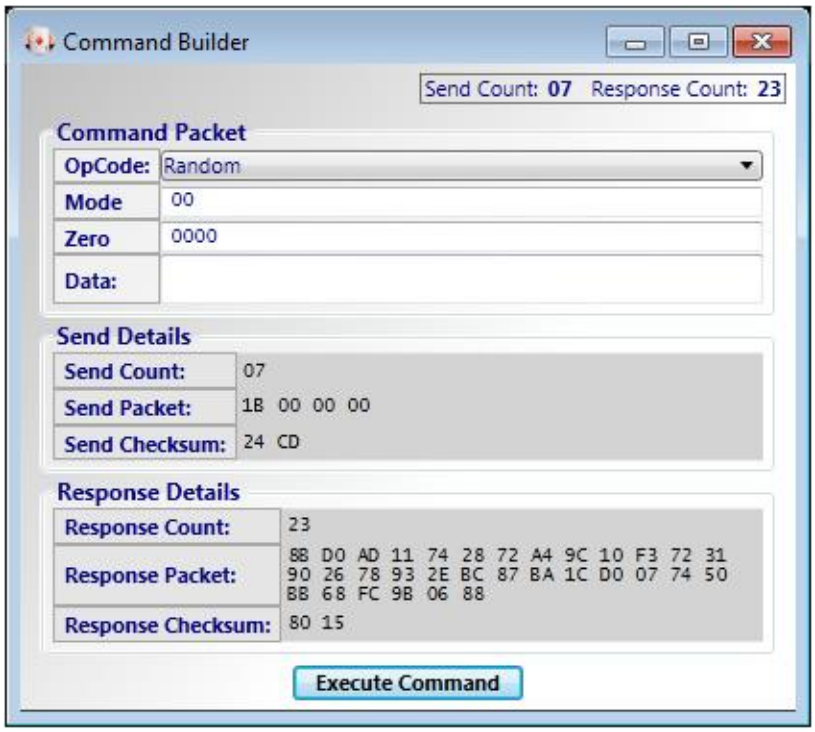
5. The lock state should now indicate locked as shown in Figure 2-5.

2.2 Random Secret Generation

The next step is to use the crypto element device to generate a 256 bit (32 byte) random number.

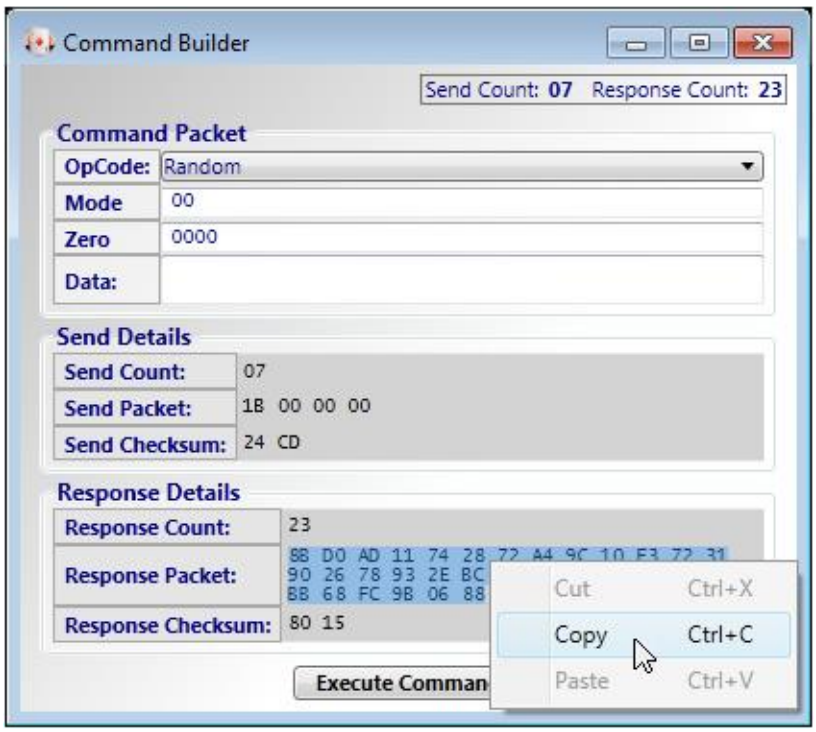
1. Run the Random command from the Command Builder dialog box.
   - Select ***Tools*** > then select ***Command Builder*** from the menu.
   - The ***Command Builder*** dialog box will be displayed as shown in Figure 2-6.
   - In the ***OpCode*** drop down list, select ***Random***.
   - Leave the ***Mode*** and ***Zero*** fields set to zeros.
   - Click on the ***Execute Command*** button.
   - The ***Response Packet*** field will contain the random number.

Figure 2-6. Random — Command Builder



2. To copy the random number, do the following:
   - Select the *random number*:
     - Left-triple-click in the ***Response Packet*** field or
     - Click and drag select the ***Response Packet*** field.
   - Right-click and select ***Copy*** as shown in Figure 2-7.
3. Every time the ***Execute Command*** button is pressed, a High-Quality True Random Number is generated.

Figure 2-7. Copy the Random Number



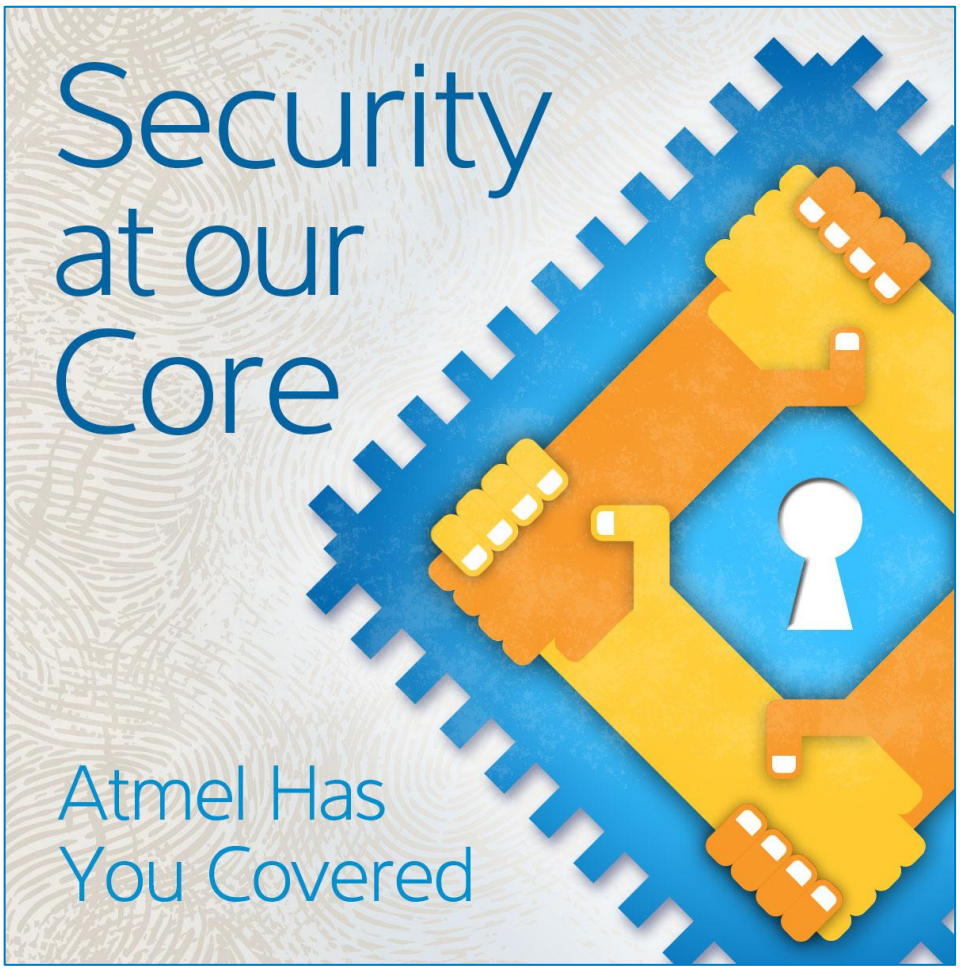
4. Paste the *random number* (which is now in the copy buffer) into any field in ACES, or it can paste into any other application. The copied *random number* will remain in the copy buffer until replaced by another Copy command.

3 Summary

Truly random secrets are extremely important to maximize the security of any system. The `Random` command implemented in both the ATSHA204A and ATECC508A generates high quality cryptographic random numbers. These True Random Numbers can be accessed for any purpose by using the ACES application software with a locked crypto element device.

4 Revision History

Doc Rev.	Date	Comments
8843B	09/2015	Updated to include all ATSHA204A, ATECC108A, and ATECC508A devices.
8843A	05/2013	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**