



Atmel AT88CKECCROOT Provisioning Root Module Kit

Introduction

The Atmel® Root Module Utility application provides an easy and secure method to create a certificate authority for provisioning the Atmel® ECC-based CryptoAuthentication™ devices. This document describes the usage for the Atmel Root Module Utility application.

Features

- Un-configured Root Module Flow to create customized Certificate Authority (CA)
- Configured Root Module Flow to create additional Root modules

Table of Contents

Un-configured Root Module Flow	3
Step 1 Start the Root Module Utility Application	3
Step 2 Insert an Un-configured Root Module	3
Step 3 Root Module License Agreement	4
Step 4 Root Module Configuration	5
Step 5 Root Module Advanced Configuration	6
Step 6 Root Module Load Backup File	7
Step 7 Configure Root Module	8
Step 8 Configure Backup Root Module	9
Step 9 Root Module Save Backup File	11
Step 10 Root Module Additional Information	12
Configured Root Module Flow	13
Step 1 Start the Root Module Utility Application	13
Step 2 Insert Configured Root Module	13
Step 3 Root Module Additional Information	14
Atmel Evaluation Board/Kit Important Notice and Disclaimer	16
Revision History.....	16

Un-configured Root Module Flow

Step 1 Start the Root Module Utility Application

Start the Root Module Utility application by selecting the Root Module Utility application from the following Microsoft Window Start Menu location:

- ▶ Select the **Start Menu > All Programs > Atmel Secure Products > Provisioning Kits > and then Root Module Utility.**

The **Atmel Root Module Utility** application window displays as shown below.

Figure 1. Root Module Utility Application Main Window



Step 2 Insert an Un-configured Root Module

1. Insert an un-configured Root Module from the AT88CKECCROOT Provisioning Root Module Kit. The Root Module is read by the Root Module Utility application and the information about the Root Module is displayed on the Root Module Utility application main window.



Keep the Root Module inserted in the computer until the Root Module configuration has been completed.

2. Select **Next >** to continue to the Root Module License Agreement.

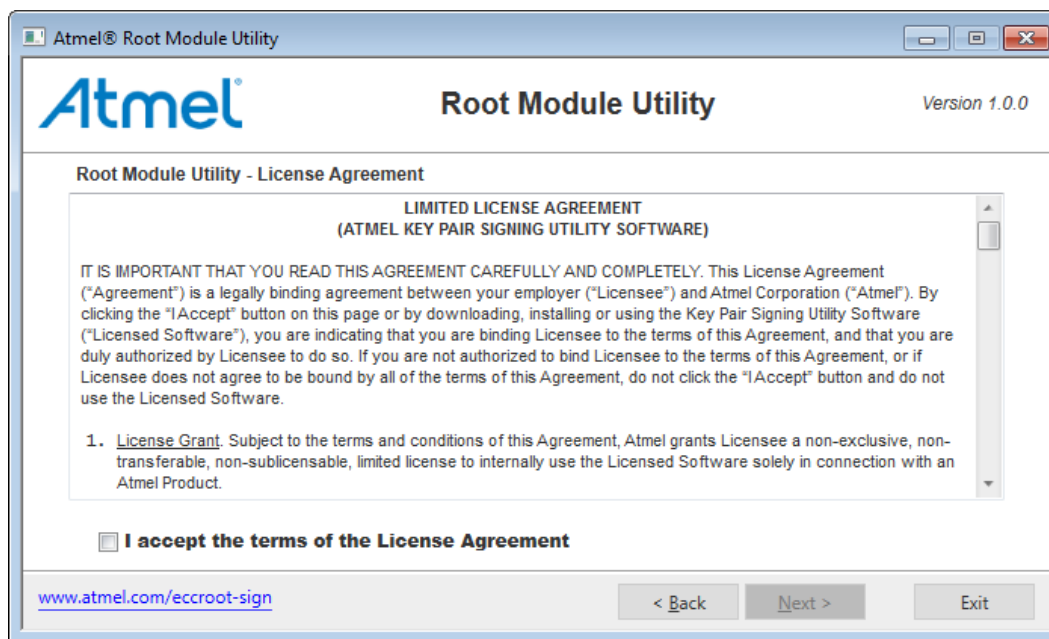
Figure 2. Sample Un-configured Root Module Main Window



Step 3 Root Module License Agreement

1. Please read the license agreement.
2. Select the check box for ***I accept the terms of the License Agreement***
3. Select **Next >** to continue to the Root Module configuration.

Figure 3. Root Module Utility License Agreement



Step 4 Root Module Configuration

1. Provide the Root Module configuration information as shown in the figure below.



Move the mouse cursor over the  image to display help information about the Root Module configuration information.

- **Module Description (Not Required)**

- The description of the Root Module to be configured. Is referenced in the future.
- Maximum length is 63 alpha-numeric characters.

- **Organization (Required)**

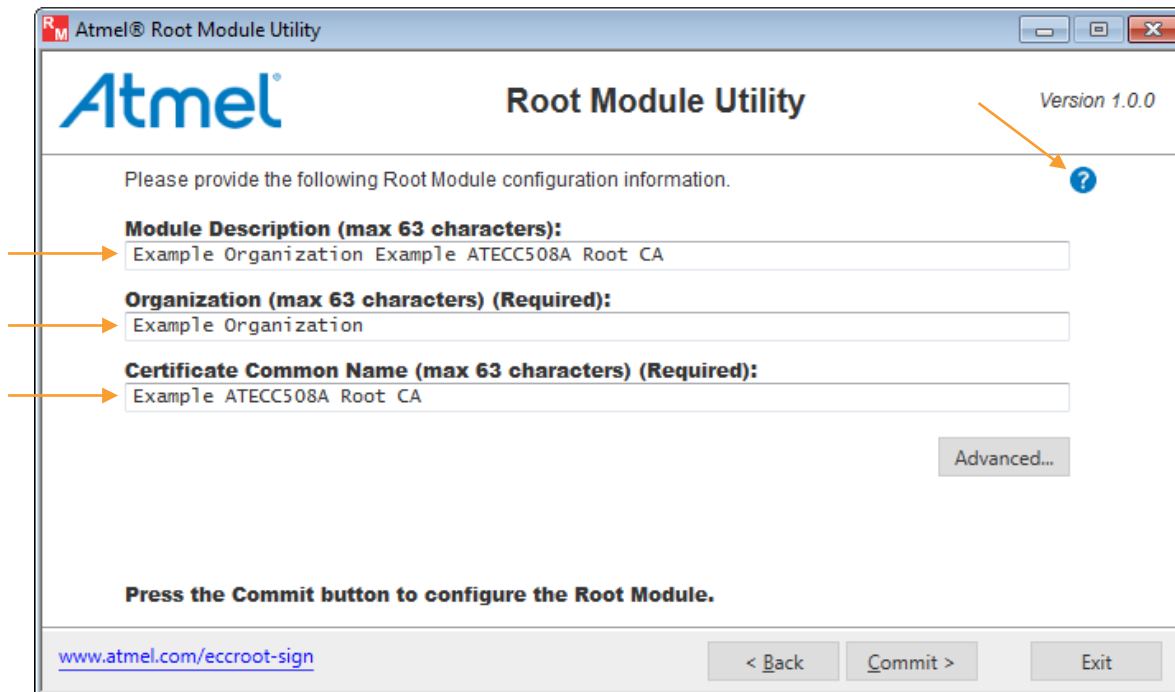
- The organization that configured the Root Module.
- The organization is added to the Root Module's Root CA X.509 certificate.
- Maximum length is 63 alpha-numeric characters.

- **Certificate Common Name (Required)**

- The Root Module certificate common name.
- The Root Module certificate common name is required for the Root Module's Root CA X.509 certificate.
- The Root Module certificate common name is used to uniquely identify the Root Module's Root CA X.509 certificate.
- Maximum length is 63 alpha-numeric characters.

2. Select the **Advanced...** to open the **Root Module Utility - Advanced Configuration Information** dialog box.
3. After entering the Root Module configuration information, select **Commit >** to configure the Root Module. See Step 7 for more information.

Figure 4. Root Module Configuration



Step 5 Root Module Advanced Configuration

Provide the following Root Module advanced configuration information.

1. Select **Load Root Module Backup File...** to load the Root Module backup file. See Step 6 for more information.



Move the mouse cursor over the  image to display help information about the Root Module private key.

- **Root Module Private Key (Required)**

- Generated by using the internal high quality random number generator within the Root Module.
- Root Module private key to be securely stored within the Root Module.
- Enter or paste a new private key into the edit box.
- Maximum length is 32 hexadecimal characters.



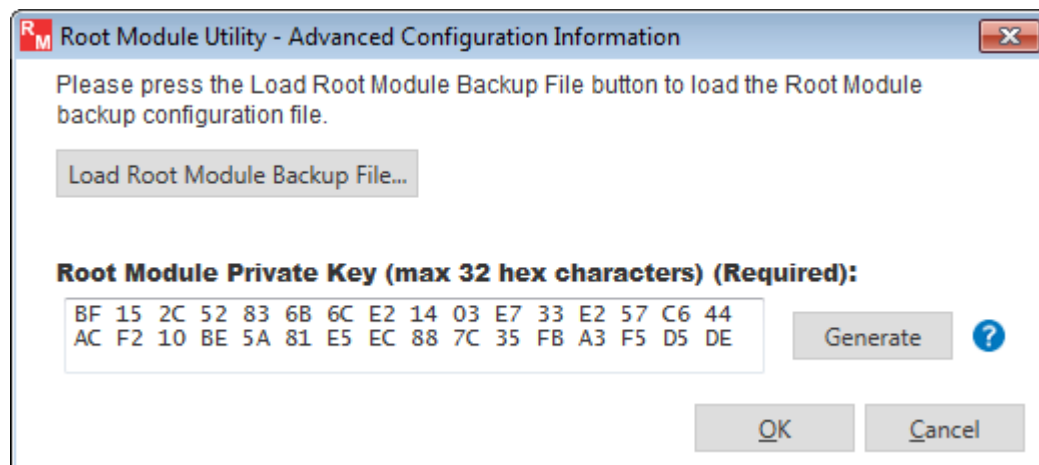
**This key is the key the entire system will be trusted to.
It is the Root of Trust.**

- **Root Module Private Key Generate Button**

- Generates a new random Root Module private key.

2. Select **OK** to save any changes to the Root Module private key.

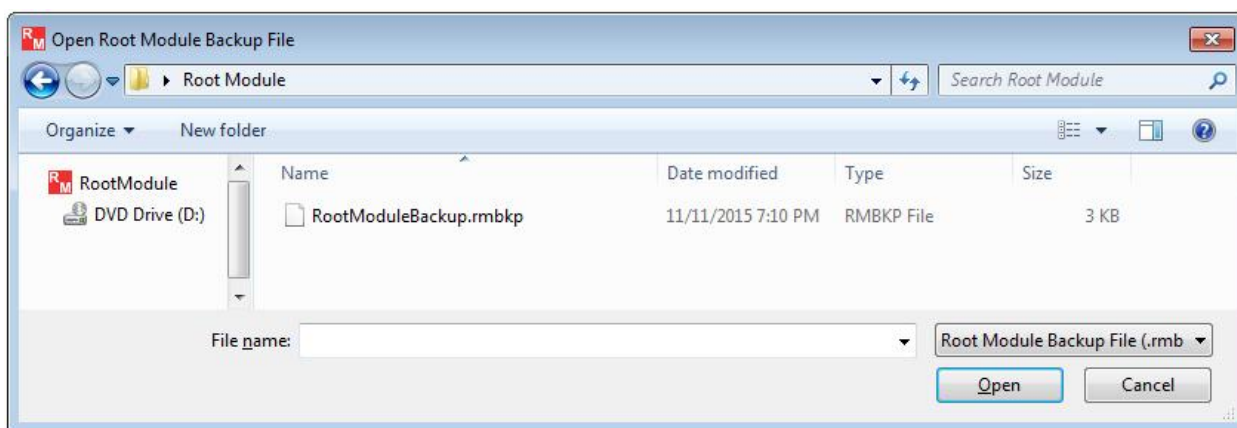
Figure 5. Root Module Advanced Configuration



Step 6 Root Module Load Backup File

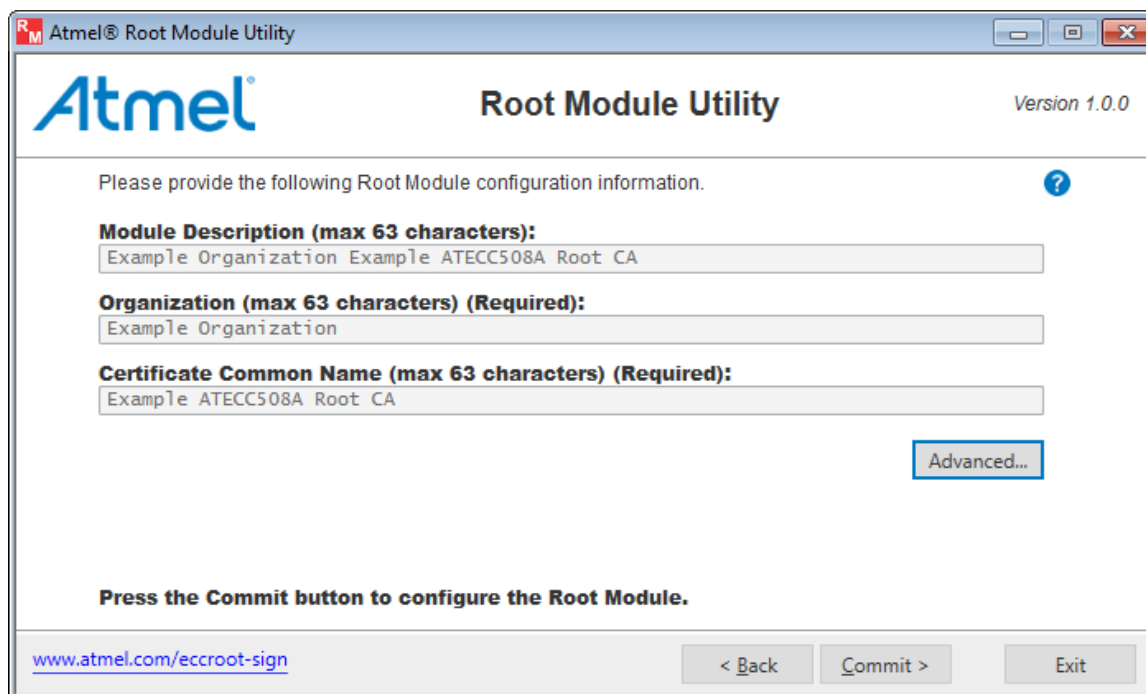
The Root Module load backup file capability is used to load a Root Module backup file to create a Root Module that is identical to the original Root Module. The original Root Module configuration process saved the backup file.

Figure 6. Example Open Root Module Load Backup File Dialog



After the Root Module load backup file has been loaded, the Root Module configuration information is loaded from the backup file, and the editable fields are disabled.

Figure 7. Example Root Module Configuration Information After The Backup File Is Loaded



Step 7 Configure Root Module

1. After entering the Root Module configuration information select **Commit** > to configure to the Root Module. The Root Module configuration process starts.



It is very important that the configured Root Module be stored in a save place. The Root Module is the trusted certificate authority within the Atmel Secure Provisioning System. Reference the application note on Best Practices to protect this valuable device.

2. Follow the directions to configure the Root Module.

Figure 8. Root Module Configuration

Figure 9. Root Module Configure Warning Dialog Box

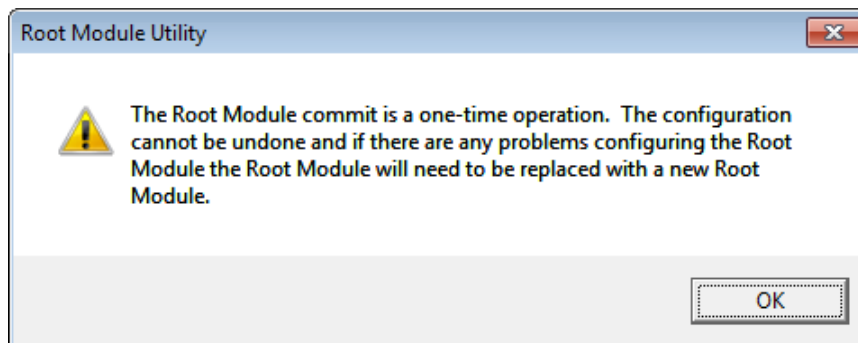


Figure 10. Root Module Configure Question Dialog Box

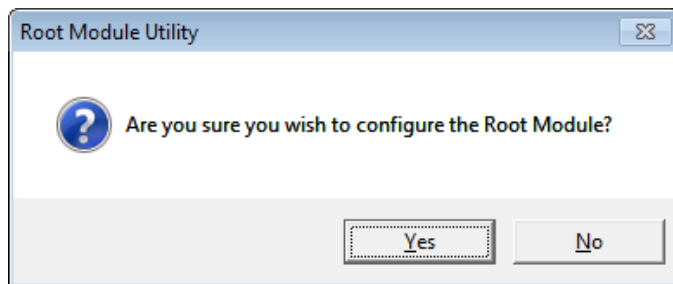
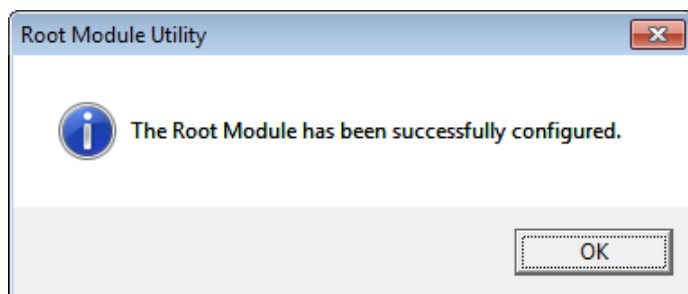


Figure 11. Root Module Successful Configuration Dialog Box



3. After the Root Module is successfully configured, it asks to configure backup Root Modules. See Step 8 for more information.
4. After a backup Root Module is configured, it asks to save the Root Module configuration file. See Step 9 for more information.
5. After the Root Module backup file is saved, options to save additional configured Root Module information are provided. See Step 10 for more information.

Step 8 Configure Backup Root Module

After the original Root Module is configured, the option to create up to 14 additional backup Root Modules is given. Atmel recommends creating at least two backups, for a total of three Root Modules. Please follow the directions carefully.



It is very important that the configured backup Root Modules be stored in a save place. The Root Module is the trusted certificate authority within the Atmel Secure Provisioning System. Reference the application note on Best Practices to protect this valuable device.



It is recommended to create a minimum of two backup Root Modules to be stored in a save place.



These backup Root Modules are identical to the original Root Module.

1. Start the backup Root Module configuration process.

Figure 12. Configure Backup Root Module Question Dialog

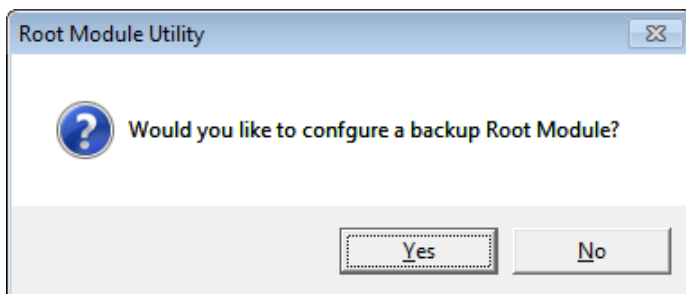
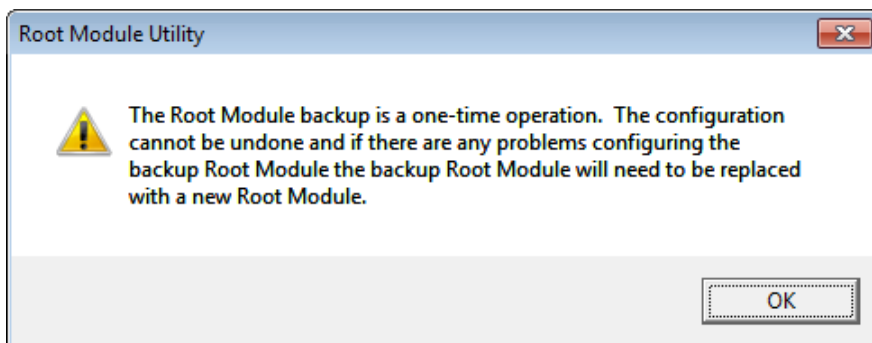


Figure 13. Backup Root Module Configure Warning



2. Insert a new un-configured Root Module before pressing the OK button

Figure 14. Insert Un-configured Root Module Dialog

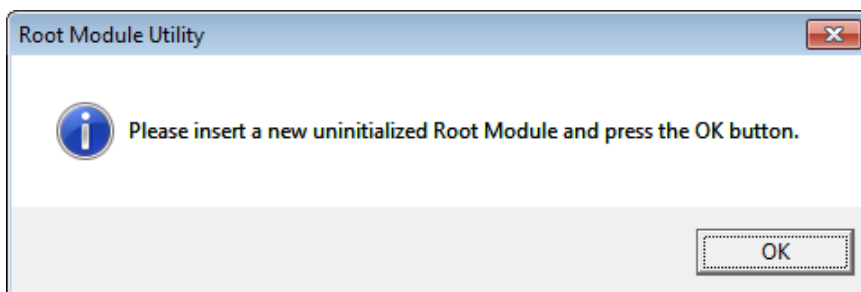
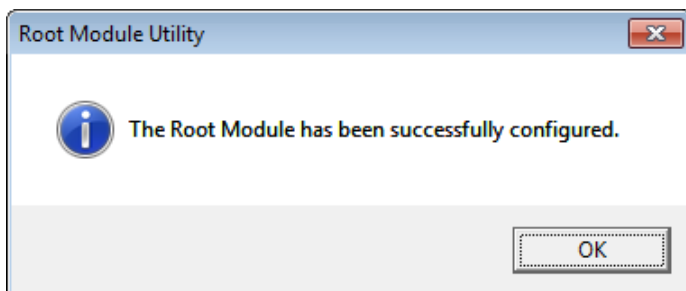


Figure 15. Root Module Successful Configuration Dialog



3. An option to create another backup Root Module is given. When the backup Root Module process is completed, the option to save the Root Module backup file is given. See Step 9 for more information.

Step 9 Root Module Save Backup File

The Root Module Save Backup File capability allows a backup file to be saved as a last resort recovery method for the Root Modules. This file is intended to be used to restore a Root Module should something happen to the original or backup Root Modules. It can also be used to create additional backup Root Modules.

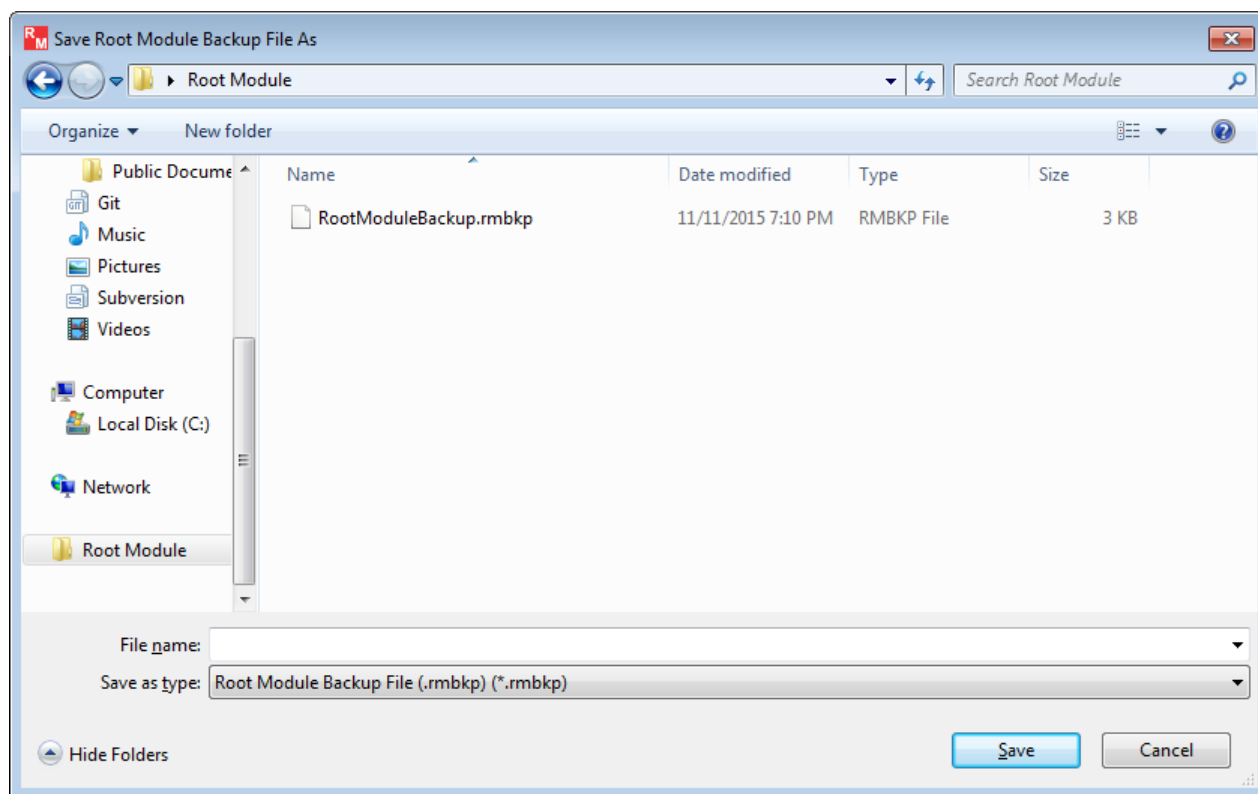


It is extremely important to save the Root Module configuration backup file. This file *cannot* be saved at a later date and time.

It is very important that the Root Module configuration file is stored in a safe place. The Root Module backup file contains sensitive information about the configuration of the Root Module. This file should not be stored on a computer, but should only exist on removable media like a USB flash drive, and that media drive secured in a safe location.

The backup file can be printed to provide a hardcopy backup. This should be kept very secure.

Figure 16. Example Save Root Module Backup File Dialog



Step 10 Root Module Additional Information

The Root Module Additional Information window allows the previous Root Module operations to be performed again if necessary and to save the Root Module's Root CA X.509 certificate.

- **Save Root Module Backup File...** button:
 - Saves the Root Module backup file. See Step 9 for more information.
- **Save Root Module Certificate File...** button:
 - Saves the Root Module Root CA X.509 certificate file. This certificate file is used to verify that a Signer Module (from the AT88CKECCSIGNER Kit) is signed by this Root Module.
- **Create Backup Root Module...** button:
 - Starts the process to create backup Root Modules. See Step 8 for more information.

Figure 17. Root Module Additional Information

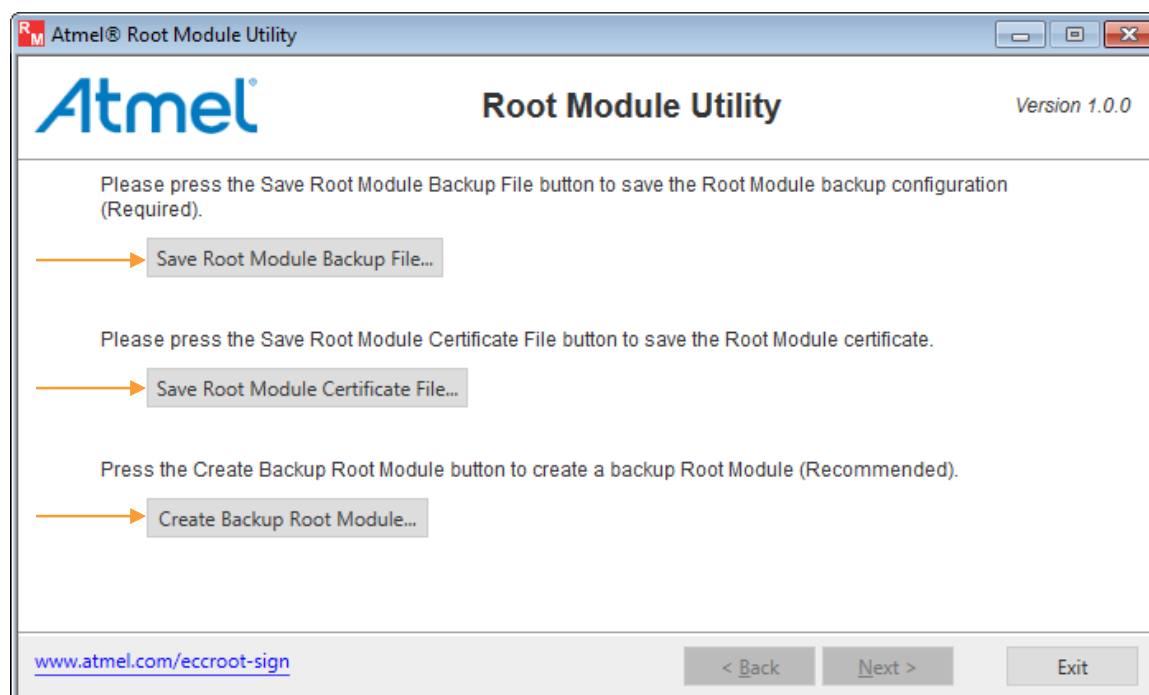
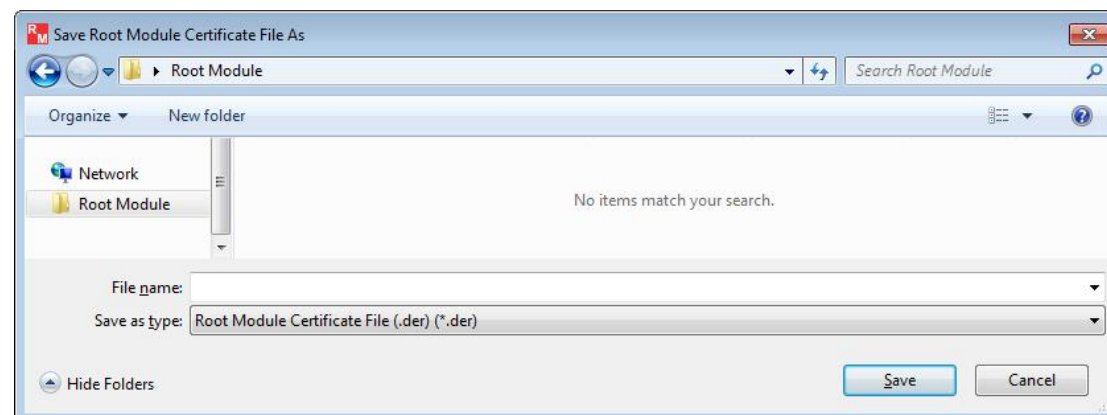


Figure 18. Example Save Root Module Certificate File



Note: This certificate file can verify that a Signer Module (from the AT88CKECCSIGNER kit) is signed by this Root Module.

Configured Root Module Flow

This section is to be used if a Root Module has already been created and want to view and/or save information about it.

Step 1 Start the Root Module Utility Application

Start the Root Module Utility application by selecting the Root Module Utility application from the Microsoft Window Start Menu location:

- ▶ Select the **Start Menu > All Programs > Atmel Secure Products > Provisioning Kits > and then Root Module Utility.**

The **Atmel Root Module Utility** window displays:

Figure 19. Root Module Utility Application Main Window



Step 2 Insert Configured Root Module

1. Insert a configured Root Module from the AT88CKECCROOT Kit.

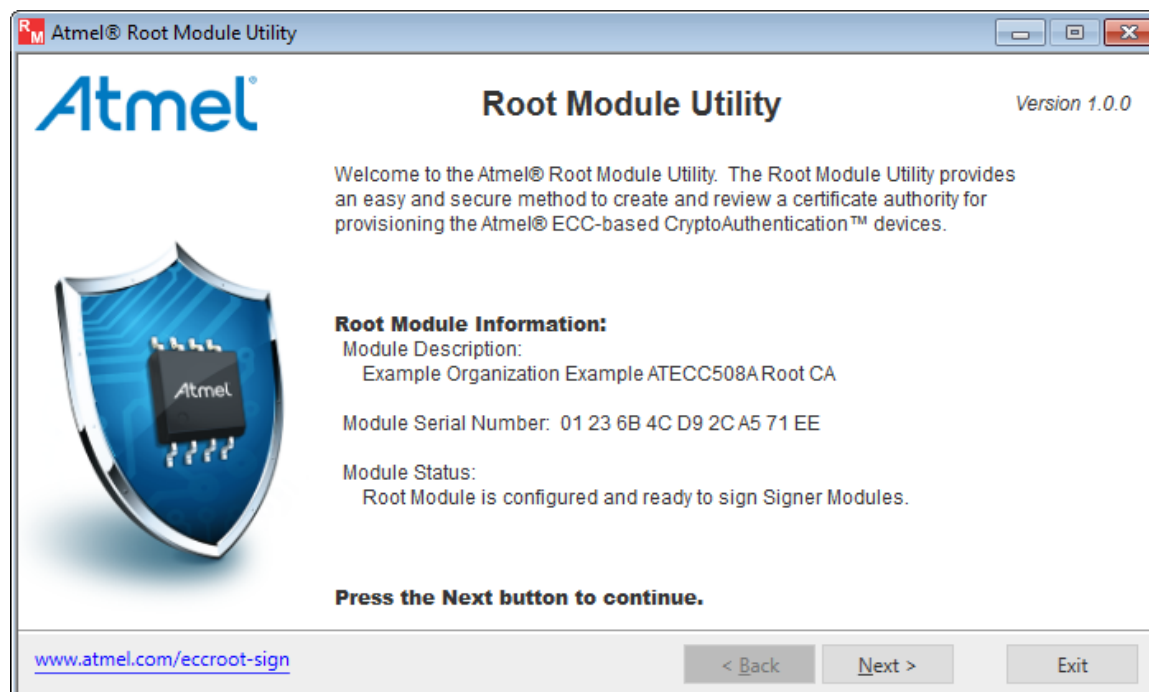
The Root Module is read by the Root Module Utility application, and information about the Root Module is displayed on the Root Module Utility application main window.



Keep the Root Module inserted in the computer until the Root Module configuration has been completed.

2. Select the **Next >** button to continue to the additional configured Root Module information.

Figure 20. Sample Configured Root Module Main Window



Step 3 Root Module Additional Information

The configured Root Module Additional Information window allows the Root Module Root CA X.509 certificate to be saved and the Root Module signer log can be viewed.

- **Save Root Module Certificate File...** button:
 - Saves the Root Module's Root CA X.509 certificate file. This file is to verify that a Signer Module (from the AT88CKECCSIGNER Kit) is signed by this Root Module.
 - The certificate is a standard X.509 DER format.
- **Root Module Signer Log Entries:** field:
 - Displays a list containing the times a Signer Module was signed by this Root Module and the associated Signer Module public key.

Figure 21. The Configured Root Module Additional Information Dialog

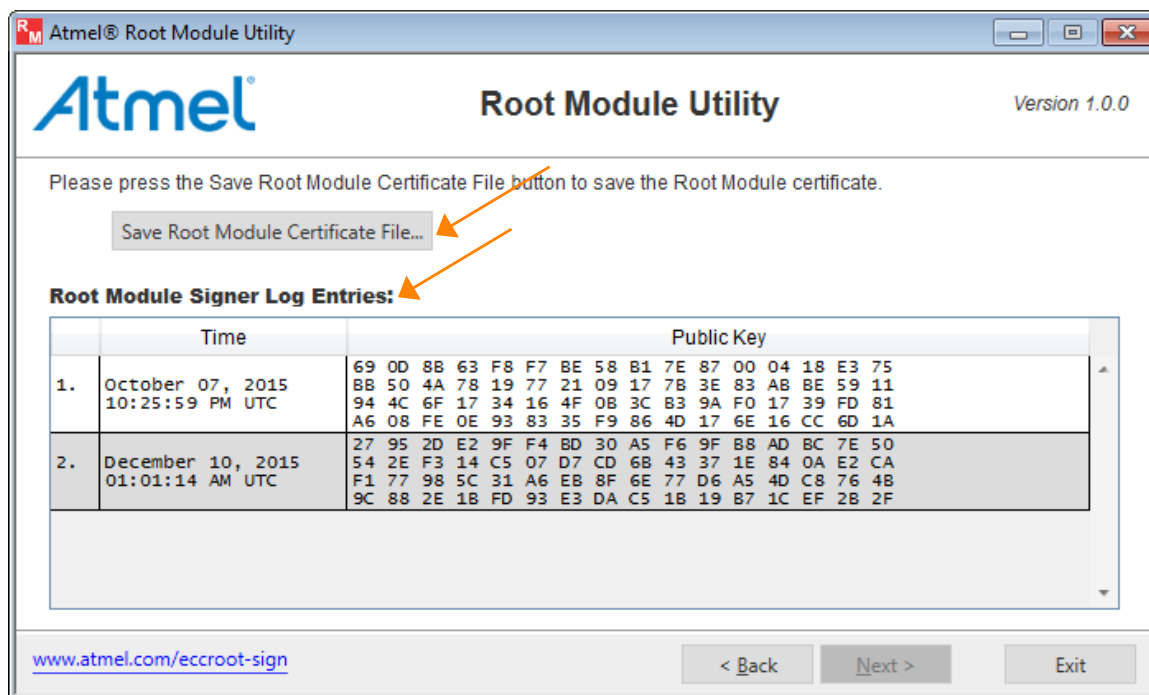
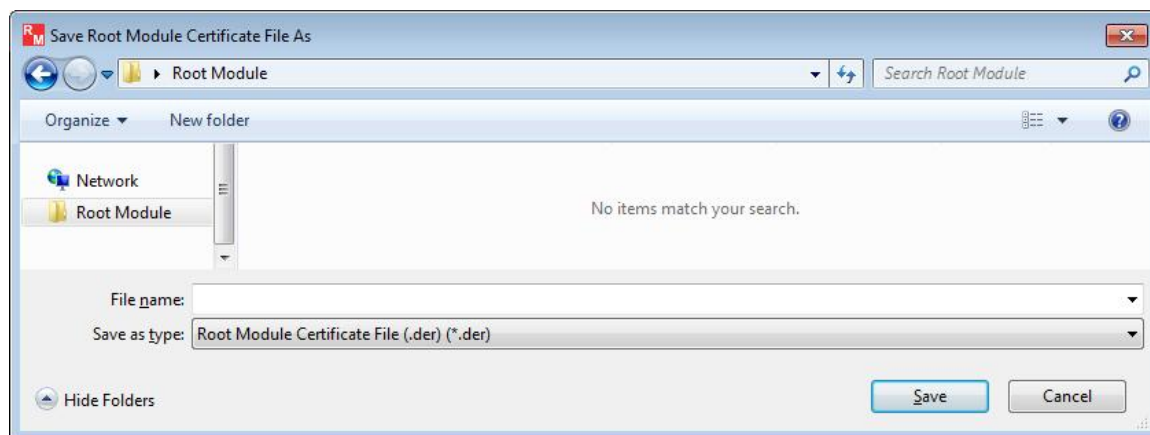


Figure 22. Example Save Root Module Certificate File Dialog



Note: This certificate file can verify that a Signer Module (from the AT88CKECCSIGNER kit) is signed by this Root Module.

Atmel Evaluation Board/Kit Important Notice and Disclaimer

This evaluation board/kit is intended for user's internal development and evaluation purposes only. It is not a finished product and may not comply with technical or legal requirements that are applicable to finished products, including, without limitation, directives or regulations relating to electromagnetic compatibility, recycling (WEEE), FCC, CE or UL. Atmel is providing this evaluation board/kit "AS IS" without any warranties or indemnities. The user assumes all responsibility and liability for handling and use of the evaluation board/kit including, without limitation, the responsibility to take any and all appropriate precautions with regard to electrostatic discharge and other technical issues. User indemnifies Atmel from any claim arising from user's handling or use of this evaluation board/kit. Except for the limited purpose of internal development and evaluation as specified above, no license, express or implied, by estoppel or otherwise, to any Atmel intellectual property right is granted hereunder. ATMEL SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RELATING TO USE OF THIS EVALUATION BOARD/KIT.

ATMEL CORPORATION
1600 Technology Drive
San Jose, CA 95110
USA

Revision History

Doc Rev.	Date	Comments
8967A	12/2015	Initial document release.

Atmel®, Atmel logo and combinations thereof, Enabling Unlimited Possibilities®, CryptoAuthentication™, and others are registered trademarks or trademarks of Atmel Corporation in U.S. and other countries. Other terms and product names may be trademarks of others.

DISCLAIMER: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. EXCEPT AS SET FORTH IN THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

SAFETY-CRITICAL, MILITARY, AND AUTOMOTIVE APPLICATIONS DISCLAIMER: Atmel products are not designed for and will not be used in connection with any applications where the failure of such products would reasonably be expected to result in significant personal injury or death ("Safety-Critical Applications") without an Atmel officer's specific written consent. Safety-Critical Applications include, without limitation, life support devices and systems, equipment or systems for the operation of nuclear facilities and weapons systems. Atmel products are not designed nor intended for use in military or aerospace applications or environments unless specifically designated by Atmel as military-grade. Atmel products are not designed nor intended for use in automotive applications unless specifically designated by Atmel as automotive-grade.