

# Implementing ZigBee Key Establishment Security with the Daintree Networks Sensor Network Analyzer

## Application Note AN027



Copyright © 2003-2008, Daintree Networks Inc  
All rights reserved

## Trademarks and acknowledgements

- ZigBee® is a registered trademark of the ZigBee Alliance.
- 802.15.4™ is a trademark of the Institute of Electrical and Electronics Engineers (IEEE).
- Pentium® is a registered trademark of Intel Corporation.
- Microsoft®, Windows®, and other Microsoft products mentioned herein are trademarks or registered trademarks of Microsoft Corporation.

These trademarks are registered by their respective owners in certain countries only. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

## Disclaimer

This note and any examples it contains are provided as-is and are subject to change without notice. Except to the extent prohibited by law, Daintree Networks makes no express or implied warranty of any kind with regard to this guide, and specifically disclaims the implied warranties and conditions of merchantability and fitness for a particular purpose. Daintree Networks shall not be liable for any errors or incidental or consequential damage in connection with the furnishing, performance or use of this guide and the examples included.

The software described in this guide is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording, for any purpose other than the purchaser's personal use, without the written permission of Daintree Networks.

Sensor Network Analyzer Release 3.0 (2009-05-21)

## Using Key Establishment

ZigBee's Smart Energy Security uses Key Establishment, which provides very strong and robust security. In fact, the security is so strong that not even sniffers (like Daintree's SNA) are able to determine the security key being used.

The high level of security is very important for applications such as Smart Energy, where sensitive information such as usage and billing must be protected.

This application note describes how to use Daintree's Sensor Network Analyzer to test your device's implementation of Key Establishment security.

## About Daintree's Sensor Network Analyzer (SNA)

The SNA combines a powerful protocol analyzer with network visualization, measurements and diagnostics for IEEE 802.15.4™ and ZigBee® applications. It provides automatic display of network formation, topology changes, and router and coordinator state changes allowing rapid detection of incorrect network behavior and identification of device or network failures.

It also provides a powerful commissioning tool that helps to hide the complexity of the underlying technology, and provides straight-forward configuration, testing and troubleshooting capabilities. Its graphical representation makes it fast and easy for installers to monitor network formation and measure key parameters such as link quality and bindings.

## About the 2400E Sensor Network Adapter

Daintree's 2400E Sensor Network Adapter can be used as an active device, which means that under the control of the SNA it is capable of active analysis.

Active devices are able to join an 802.15.4 or ZigBee network, interact with other devices on it, and actively poll devices to gain information not available through passive sniffing alone. They can also issue commands to network devices, such as configuration settings during commissioning, as described in this application note.

Visit [www.daintree.net](http://www.daintree.net) to find out more about Daintree products.



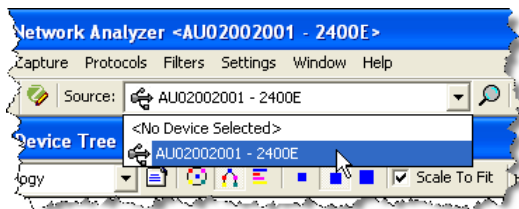
## Testing Key Establishment security

You can use the Professional edition of the SNA along with an active device (Daintree's SNA, Ember's EM250 or an Integration ZigBee dongle) to test your device's implementation of Key Establishment security. This application note shows you how to

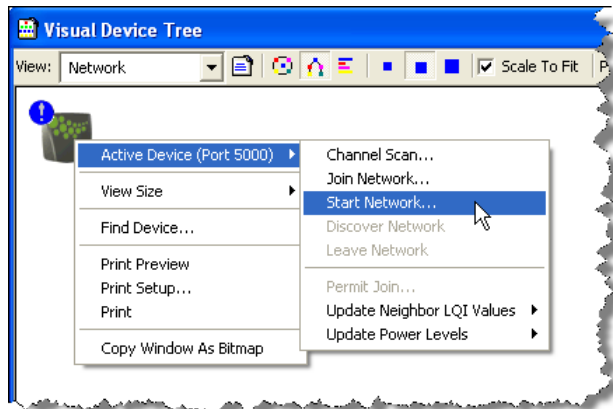
- Start a network using Key Establishment
- Add or remove Link Keys on a Trust Center while the network is running
- Join a network using Key Establishment
- Re-join a network using Key Establishment
- Passively sniff traffic using Network and Link Keys

## Start a network using Key Establishment

1. Connect to an active device (Daintree 2400E, Ember EM250, or Integration ZigBee dongle), and select it from the **Source** list. (See the SNA's online help if you need more detailed instructions.)



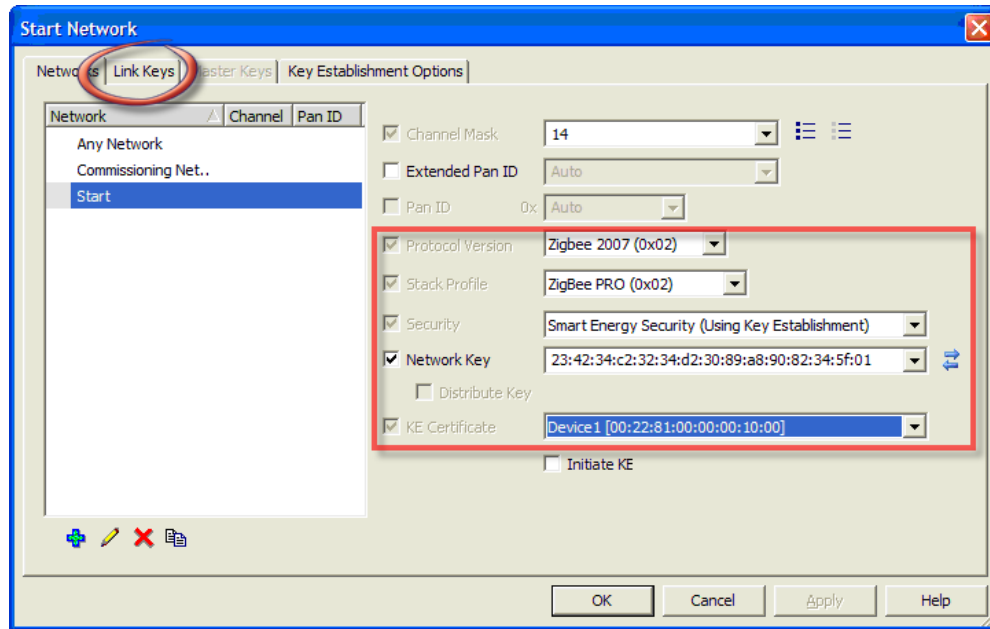
2. On the Visual Device Tree, right-click the active device, and then select **Active Device > Start Network**.




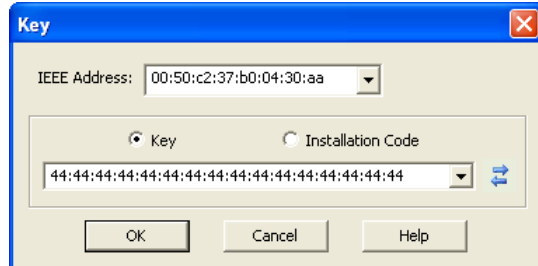
3. On the Start Network dialog box, enter details about the network to start:
  - Choose the appropriate **Channel Mask**. If you would like to specify the **Extended Pan ID** enter it here, otherwise it will be assigned automatically.
  - For Key Establishment, set **Protocol Version** to **ZigBee 2007 (0x02)**, the **Stack Profile** to **ZigBee PRO (0x02)**, and **Security** to **Smart Energy Security (Using Key Establishment)**.
  - If you would like to specify the **Network Key** enter it here, otherwise it will be created automatically.

## Implementing ZigBee Key Establishment Security with the Daintree SNA

- Select any **Certificate** from the drop-down list. This assigns an IEEE address to the device, as well as matching Certicom security information.



4. Click the **Link Keys** tab.
5. For each device that will be joining the network, click , and then enter the device's IEEE address and Link Key (MSB first order). Then click **OK**.



6. On the Start Network dialog box, click **OK** to start the network using the specified settings.

## Notes

Please be aware of the following requirements:

### Multiple SNA instances


If you are running two instances of the SNA (one as the coordinator and one as the joining device), the certificate you choose must be unique on the network. If you are using the Daintree 2400E or Integration dongle as your active device, the MAC is over-written to match the certificate.

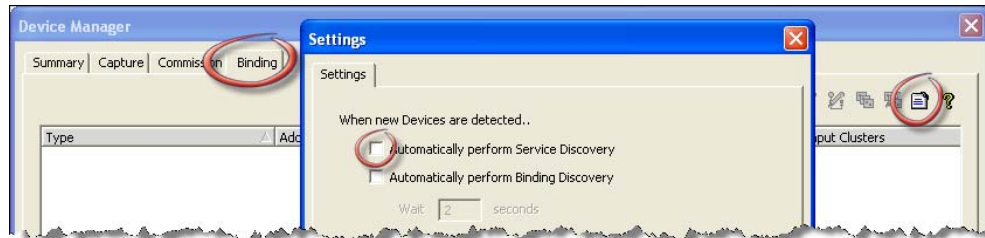
### Integration ZigBee dongle

If you are using an Integration ZigBee dongle as your active device, you need a second dongle to act as a capture device to be able to see the packets sent and received.

## Ember EM250

If you are using an Ember EM250 as your active device, you need to turn off automatic service discovery before starting the network:

1. From the SNA's **Settings** menu, select **Device Manager**.
2. On the Device Manager dialog box, select the **Binding** tab, and then click  (Settings).
3. On the Settings dialog box, make sure **Automatically perform Service Discovery** is not selected. Then click **OK**.

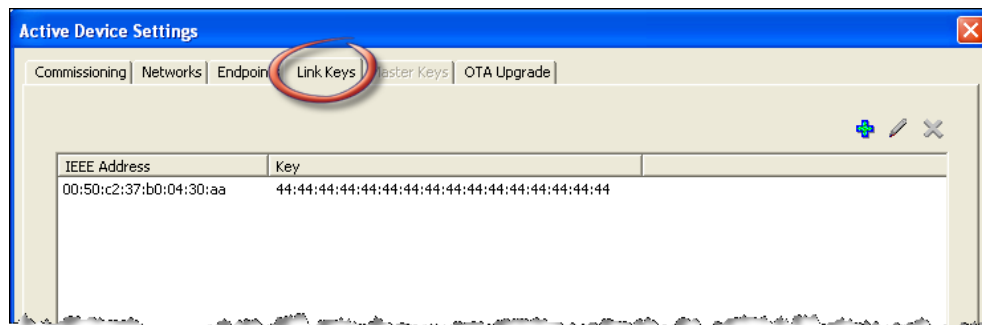



## Add or remove Link Keys on a Trust Center while the network is running



1. From the SNA's **Settings** menu, select **Device Manager**, or click the Device Manager icon from the main SNA toolbar.



2. Select the **Commission** tab, which shows a list of all devices on the network.
3. Double-click the device acting as the network's Trust Center to edit its settings.
4. On the Active Device Settings dialog box, select the **Link Keys** tab.



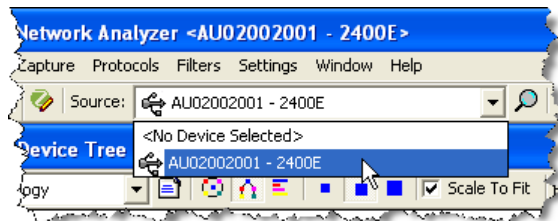
5. Edit Link Key settings as required:
  - o Click  to add a new Link Key. You will need to enter the IEEE address of the device that will be joining the network, as well as a Link Key for it to use when communicating with the Trust Centre.

- Select an existing Link Key and click  to edit its details.
- Select an existing Link Key and click  to delete its details.

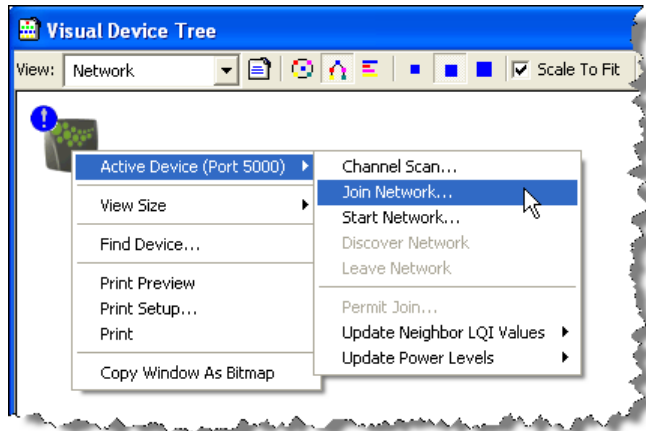
## Join a network using Key Establishment

Note that the IEEE address and key of the joining device on the network must already be configured in the Trust Center.

1. Connect to an active device (Daintree 2400E, Ember EM250, or Integration ZigBee dongle), and select it from the **Source** list. (See the SNA's online help if you need more detailed instructions.)

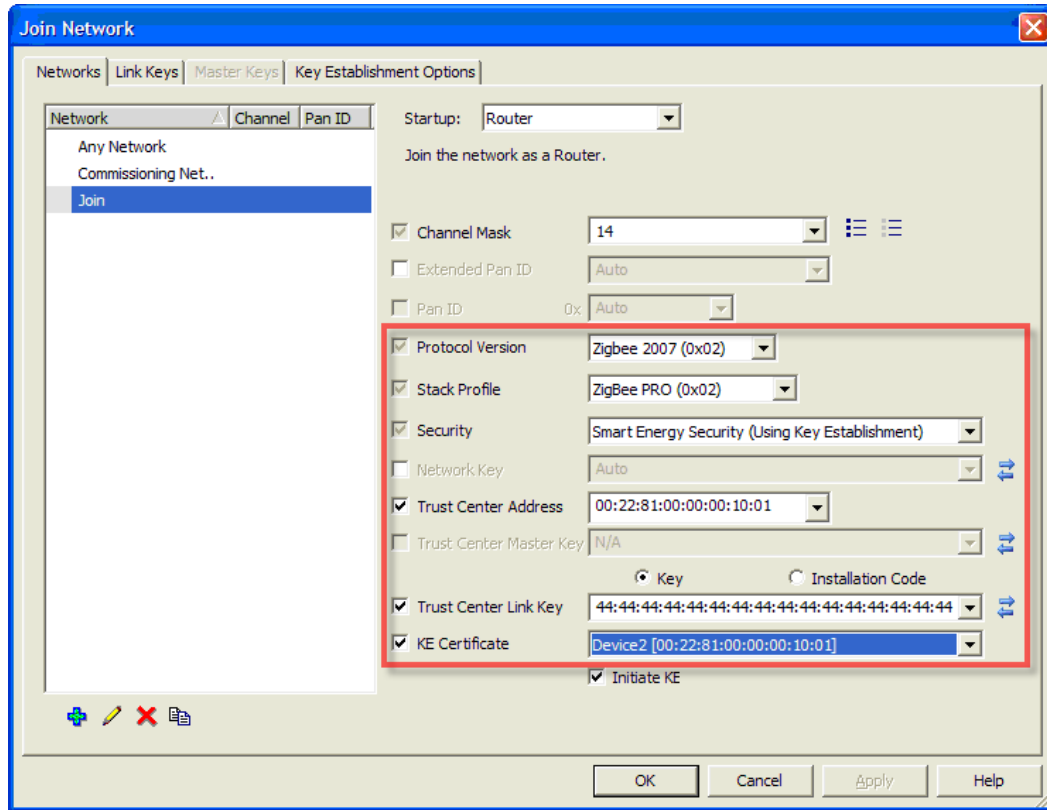


2. On the Visual Device Tree, right-click the active device, and then select **Active Device > Join Network**.



3. On the Join Network dialog box, enter details about the network to join:
  - Choose the appropriate **Channel Mask**. If you would like to specify the **Extended Pan ID** enter it here, otherwise it will be assigned automatically.
  - For Key Establishment, set **Protocol Version** to **ZigBee 2007 (0x02)**, the **Stack Profile** to **ZigBee PRO (0x02)**, and **Security** to **Smart Energy Security (Using Key Establishment)**.
  - Select **Trust Center Address**, and then enter the IEEE address of the Trust Center (usually the coordinator).
  - Select **Trust Center Link Key**, and then enter the Link Key (MSB first) that has been configured in the Trust Center for this device.
  - Select the **Certificate** you want to use from the drop-down list. This assigns a MAC address to the device, as well as matching Certicom security information.

## Implementing ZigBee Key Establishment Security using Daintree's SNA




4. Click **OK** to join the network as specified.

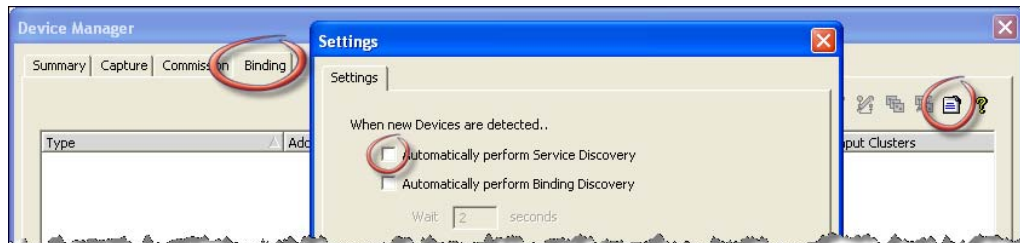
## Notes

Please be aware of the following requirements:

### Ember EM250

You need to turn off automatic service discovery before joining the network:



1. From the SNA's **Settings** menu, select **Device Manager**.
2. On the Device Manager dialog box, select the **Binding** tab, and then click  (Settings).
3. On the Settings dialog box, make sure **Automatically perform Service Discovery** is not selected. Then click **OK**.

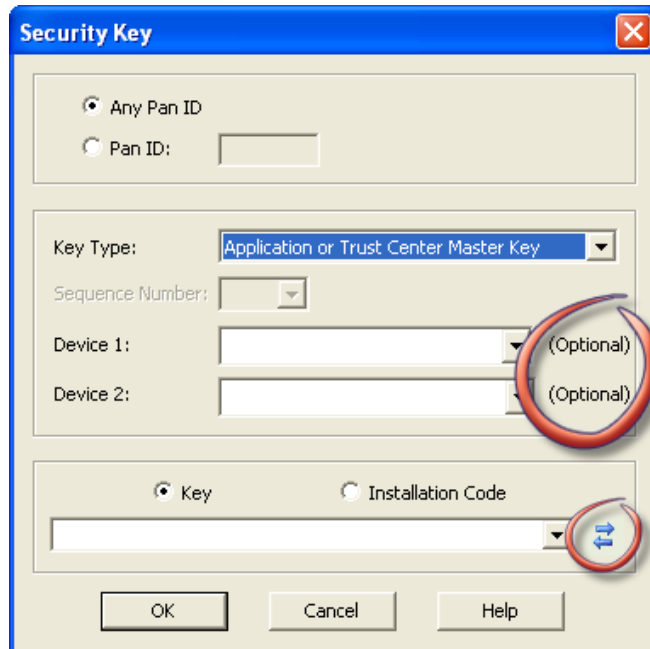


If you are using an Ember EM250 as your active device, you do not need to specify the Trust Center address when joining the network.



## Passively sniff traffic using Network and Link Keys

1. Connect to a capture device and start capturing on the required channel. (See the SNA's online help if you need more detailed instructions.)
2. From the SNA's **Settings** menu, select **Options**.
3. On the Options Dialog box, click the **Security** tab, and then click  to create new Network and Link security keys.
4. Enter details about the security keys:
  - o Specifying the IEEE addresses is optional.
  - o Multiple keys per device pair are supported.
  - o The SNA requires keys to be entered MSB first. You can click  to reverse the order of keys entered with LSB first.



5. Click **OK** to save the security key details.

## Automatic discovery of keys

Network and Link security keys are often shared over the air using Transport-Key messages. The SNA can discover these keys automatically, and store their details in its Security Key database.

## Key Establishment security

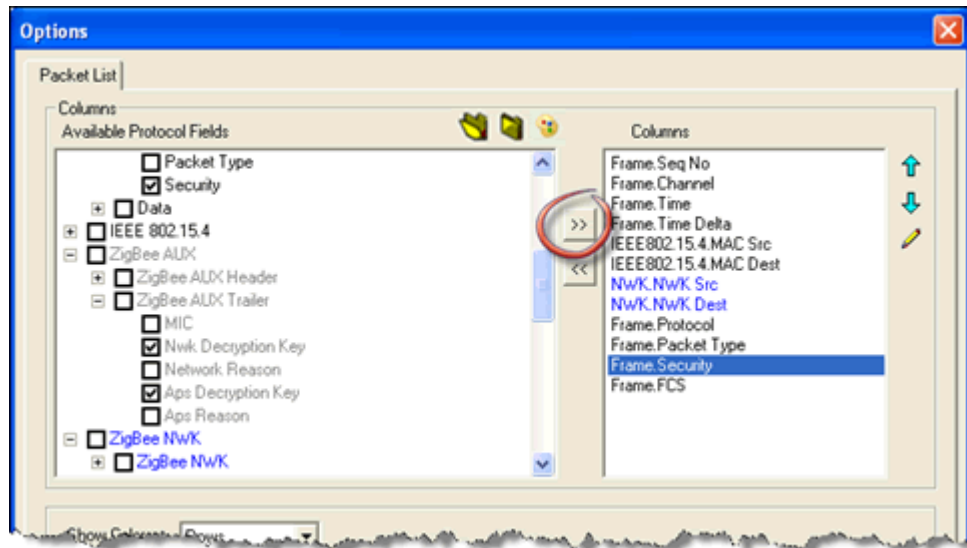
As part of the Key Establishment procedure, the Trust Center changes the Link Keys used by devices. The nature of this type of security means that the SNA is unable to determine the updated Link Key automatically. Therefore, it must be entered manually using the steps described above.

## Viewing security details

After the SNA has populated its Security Key database, through both manual entries and automatic discovery as described above, it displays the decoded messages in the Packet List window, with the type of security used shown in the right-hand column.

If required, you can also show the security key used to decode each packet:

1. From the SNA's **Settings** menu, select **Options**.
2. Click the **Packet List** tab, and then select each of the security information columns you want displayed. For example
  - o Frame > Frame > Security
  - o ZigBee AUX > ZigBee AUX Trailer > Nwk Decryption Key
  - o ZigBee AUX > ZigBee AUX Trailer > Aps Decryption Key



3. Click **>>** to add the selected fields to the list of Columns to display in the Packet List window. You can also use **↑** and **↓** to change the order in which columns are displayed.
4. Click **OK** to save your settings.

## Security certificates

The certificates provided with the SNA are suitable for test networks only.

Before you can use security with a live network, you need to add details of your own security certificates to the **Certificates.xml** file (in the **Daintree Networks/Sensor Network Analyzer** directory).

```
<entry name="Device1 [00:22:81:00:00:00:10:00]">
  <value name="IEEE Address">
    0022810000001000</value>
  <value name="CA Public Key">
    0200fde8a7f3d1084224962a4e7c54e69ac3f04da6b8</value>
  <value name="Certificate">
    0307267bd9f3cec3d52cfb0164e09d1e9cac4848421a0022810000001000544553
    545345434101090001000000000000</value>
  <value name="Private Key">
    00b5b55cb997095c34934f63deff1e78d51fc455f9</value>
  <value name="Public Key">
    030354f85d7ed6e6f58061c448e1af0c8a9599a94bfb</value>
</entry>
```

1. Open the **Certificates.xml** file using an XML editor.
2. Create a new entry for each of your security certificates in the format shown above:
  - o Specify the **<entry name>** by which the security certificate details will be identified. This is the name that is displayed in the SNA's **KE Certificate** list.
  - o Enter all other values as per your Certicom security certificates.
3. Save your changes, and then start (or re-start) the SNA. This causes the SNA to load the updated details from the **Certificates.xml** file and make the new certificates available for selection when you start and join networks.