

Using eCM Manager to Create and Write Signing Keys

Follow these steps to create a new signing key and transfer it to an eSlate Cryptographic Module.

1. Open eCM Manager.
2. Plug an eCM into a USB port on the computer.
3. Open eCM Manager.
4. Plug an eCM into a USB port on the computer.
5. In the **Key ID** field, enter an ID for the eCM, using a number from 1 to 99. (The Key ID **MUST** be the same for all eCMs used in an election).
6. Click the **New Signing Key** button.
7. In the **PIN** field, enter a PIN (password) of 6-12 letters and/or numbers. This is case sensitive.
8. Repeat the PIN in the **Confirm** field.
9. Click the **Write Module** button and respond to any messages that appear.
10. Note the eCM **Serial No.** field display.
11. Remove the eCM, label it for the election, and record the serial number and PIN in a secure location.
12. When finished writing eCMs, click the **Save File** button and follow the prompts to save the module data to the desired location on your PC. This data can be used to create more eCMs for this election or to verify existing eCMs. *You must save before exiting eCM Manager.*
13. Record the name of the .eCM file and the date saved.
14. Back up the .eCM file to CD.
15. Store labeled eCMs in a secure location.

(Continued on following page)

Other eCM Manager Features

To write from one eCM to another

This procedure can be used to create additional eCMs if the .eCM file was not saved before exiting eCM Manager:

1. Open eCM Manager.
2. Insert the source eCM into the USB port.
3. Enter the eCM PIN.
4. Click the **Read Module** button.
5. Remove the source eCM from the USB port.
6. Insert the target eCM into the USB port.
7. Confirm the PIN *OR* enter a new eCM PIN and confirm.
8. Click the **Write Module** button.
9. Remove and label the new eCM.

To write an eCM from a saved .eCM file

1. Open eCM Manager.
2. Click the **Open File** button.
3. Navigate to the saved .eCM file.
4. Confirm the PIN *OR* enter a new eCM PIN and confirm.
5. Insert an eCM into the USB port.
6. Click the **Write Module** button.
7. Remove and label the new eCM.

To verify the signing key on an eCM token against a saved .eCM file

1. Open the eCM Manager.
2. Insert the eCM to be verified into the USB port.

Election Solutions

Knowledge Base



Article #1 In a Series

3. Click the **Open File** button to open the .eCM file.
4. Click the **Verify Module** button. A dialog box appears either confirming a match or identifying a mismatch.
5. If there is a match, remove and label the eCM and make sure the eCM Key ID and PIN are logged in a secure location.

Best Practices for eCM Management

- Before creating eCMs for an election, determine whether one PIN will be used for all eCMs for the election, or if each eCM will have its own unique PIN.
- Label eCM tokens with a recognizable notation (e.g., jurisdiction name), but not with the eCM Key ID, Key GUID, or PIN.
- Log and track the number of eCMs created, eCM serial numbers, and eCM PIN(s) and the individuals they are assigned to, and keep this information in a secure location.