## Host Transfer-of-Ownership Sequence

The following sequence must be issued by the current owner to the Soteria-G3 code to transfer ownership to either a new owner or intermediate entity.

### Sequence for Current Owner to Transfer Ownership

In this sequence the current owner transfers ownership to the new owner.

Host Sequence:

1. Get current owner state
   1. Host issues Primary Owner Container Status (0100b) command
   2. If any containers are invalid, abort transfer and fix issues.
2. Gets and save a copy of Primary Owner Container
   1. Host issues Get Primary Owner Container (1000b)
   2. If the command does not complete successfully, abort the transfer-of-ownership sequence and fix issues
3. Enable Owner Crisis Command Interface
   1. Host issues Get Random Value (0110b)
   2. Host issues Hash of Primary Owner Container (0011b)
   3. Host generates and issues Signed Enable Unrestricted Transfers command (0111b)
      1. Sets Owner Configuration Bit [1] Unrestricted Transfer of Ownership Enable = 1
      2. Sets Owner Configuration Bit [2] Crisis Command Interface =1
      3. OTAKpub key not required
4. Check if Owner Crisis Interface enabled
   1. Host issues Primary Owner Container Status (0100b) command
   2. Verify Owner Configuration Bits [2:1] = 11b
      1. If Owner Configuration Bits [2:1] != 11b, abort the transfer-of-ownership sequence and fix issues
5. Current Owner Transfers Ownership
   1. Gets Current Owner Container RPMC value (0101b)
   2. Execute Transfer-of-Ownership Command. Inserts CCKpub key(s) provided by new owner
   3. Gets Current Owner Container RPMC value (0101b)
      1. If RPMC value incremented, transfer completed successfully
      2. If RPMC value not incremented, transfer did not complete successfully.
         1. Host must issue Primary Owner Container Status (0100b) command to debug issue
6. Power down machine and ship to new owner or intermediate entity
   1. Note that any of the current owner secrets stored on device should be destroyed before shipping machine.
7. New owner Configures Machine
   1. If no valid EC\_FW present, the new owner must use the Boot ROM crisis port to program EC\_FW image into internal SPI Flash
   2. If valid EC\_FW present and AP\_FW not valid, the new owner may update the EC\_FW images using MCTP-PLDM commands via crisis port
   3. If no valid AP\_FW present, the new owner may use the SG3 AP\_FW image restore commands supported over MCTP – PLDM commands.

### Sequence for New Owner to Transfer Ownership

In this sequence the current owner enables the device so the new owner can execute the transfer of ownership command.

Host Sequence:

1. Get current owner state
   1. Host issues Primary Owner Container Status (0100b) command
   2. If any containers are invalid, abort transfer and fix issues.
2. Gets and save a copy of Primary Owner Container
   1. Host issues Get Primary Owner Container
   2. If the command does not complete successfully, abort the transfer-of-ownership sequence and fix issues
3. Enable Owner Crisis Command Interface
   1. Host issues Get Random Value (0110b)
   2. Host issues Hash of Primary Owner Container (0011b)
   3. Host generates and issues Signed Enable Unrestricted Transfers command (0111b)
      1. Sets Owner Configuration Bit [1] Unrestricted Transfer of Ownership Enable = 1
      2. Sets Owner Configuration Bit [2] Crisis Command Interface =1
      3. Inserts OTAKpub key provided by new owner or intermediate entity
4. Check if Owner Crisis Interface enabled
   1. Host issues Primary Owner Container Status (0100b) command
   2. Verify Owner Configuration Bits [2:1] = 11b
      1. If Owner Configuration Bits [2:1] != 11b, abort the transfer-of-ownership sequence and fix issues
5. Power down machine and ship to new owner or intermediate entity
   1. Note that any of the current owner secrets stored on device should be destroyed before shipping machine.
6. Entity Receiving Machine
   1. If New owner
      1. Gets Current Owner Container RPMC value (0101b)
      2. Execute Transfer-of-Ownership Command
      3. Gets Current Owner Container RPMC value (0101b)
         1. If RPMC value incremented, transfer completed successfully
         2. If RPMC value not incremented, transfer did not complete successfully.
            1. Host must issue Primary Owner Container Status (0100b) command to debug issue
   2. If Intermediate Entity
      1. Gets OTAKpub key from new owner
      2. Executes Update OTAK Key command to insert new owner’s OTPpub key
      3. <Return to step 5>

## Transfer-of-Ownership Scenarios

This section describes the various transfer-of-ownership scenarios supported by the SG3 code.

Terminology:

* Current Owner = Owner A
* New Owner = Owner B

There are two types of ownership transfers:

* Direct: Owner A -> Owner B
* Indirect: Owner A -> Intermediate Entity -> Owner B

There are three methods supported for transferring ownership:

* Current Owner Performs the Transfer-of-Ownership on Behalf of the New Owner
* Current Owner Enables New Owner to Perform the Transfer-of-Ownership
* Current Owner Enables Trusted Intermediate Entity to Enable New Owner to Perform the Transfer-of-Ownership

The following sections describe the sequence options for supporting the transfer options.

### Current Owner Performs the Transfer-of-Ownership on Behalf of the New Owner

Transfer Type: Owner A -> Owner B

Sequence Steps:

1. Owner B provides the following to the Owner A
   1. Owner Container parameters required for Transfer-of-Ownership command
   2. (optional) Image KHB and TAGx image
2. Owner A prepares machine for transfer (e.g., removes owner secrets)
   1. (optional) Restores signed OEM images
3. Owner A executes Enable Unrestricted Transfers command to enable I2C crisis interface to process ownership commands.
4. Owner A creates and signs Transfer-of-Ownership command using Owner A Container Command private key (CCKx private key)
5. Owner A executes Transfer-of-Ownership command
6. Owner A ships machine to Owner B
7. Owner B is current owner
   1. Owner B can update images as needed
      1. If no valid images, Owner B can use the Boot ROM crisis port for updating images in internal flash
      2. If valid SG3 code found, Owner B can use the SG3 I2C commands to update EC\_FW.

### Current Owner Enables New Owner to Perform the Transfer-of-Ownership

Transfer Type: Owner A -> Owner B

Sequence Steps:

1. Owner B provides the following to the Owner A
   1. OTAKpub key required for signing Transfer-of-Ownership command
   2. (optional) Image KHB and TAGx image
2. Owner A prepares machine for transfer (e.g., removes owner secrets)
   1. (optional) Restores signed OEM images
3. Owner A executes Enable Unrestricted Transfers command to add OTAKpub key to Owner Container and enable I2C crisis interface to process ownership commands.
4. Owner A ships machine to Owner B
5. Owner B creates and signs Transfer-of-Ownership command using Owner B Owner Transfer Authorization private key (OTAK private key)
6. Owner B executes Transfer-of-Ownership command
7. Owner B is current owner
   1. Owner B can update images as needed
      1. If no valid images, Owner B can use the Boot ROM crisis port for updating images in internal flash
      2. If valid SG3 code found, Owner B can use the SG3 I2C commands to update EC\_FW.

Note: See section 6.6.2 Sequence for New Owner to Transfer Ownership for the detailed host command sequence.

### Current Owner Enables Trusted Intermediate Entity to Enable New Owner to Perform the Transfer-of-Ownership

Transfer Type: Owner A -> Intermediate Entity -> Owner B

Sequence Steps:

1. Trusted Intermediate Entity provides the following to the Owner A
   1. OTAKpub key required for signing Update OTAK Key command
2. Owner A prepares machine for transfer (e.g., removes owner secrets)
   1. (optional) Restores signed OEM images
3. Owner A executes Enable Unrestricted Transfers command to add OTAKpub key to Owner Container and enable I2C crisis interface to process ownership commands.
4. Owner A ships machine to Trusted Intermediate Entity
5. Owner B provides the following to the Trusted Intermediate Entity
   1. OTAKpub key required for signing Transfer-of-Ownership command
6. Trusted Intermediate Entity uses the Update OTAK Key command to insert Owner B OTAKpub key into owner container.
7. Trusted Intermediate Entity ships machine to Owner B
8. Owner B creates and signs Transfer-of-Ownership command using Owner B Owner Transfer Authorization private key (OTAK private key)
9. Owner B executes Transfer-of-Ownership command
10. Owner B is current owner
    1. Owner B can update images as needed
       1. If no valid images, Owner B can use the Boot ROM crisis port for updating images in internal flash
       2. If valid SG3 code found, Owner B can use the SG3 I2C commands to update EC\_FW.

Note: See section 6.6.2 Sequence for New Owner to Transfer Ownership for the detailed host command sequence.