9. Compatibility

The ATSHA204 is designed to be upwards compatible with the AT88SA102S for field operation. Most systems designed to use the AT88SA102S in Client devices will work perfectly with the ATSHA204 in the Client devices without any modification to the Host system software or hardware.

Host systems that utilize the AT88SA10HS Host device will also interoperate properly with the ATSHA204 Client device in place of a previously used AT88SA102S Client; however, the AT88SA10HS itself cannot be replaced with the ATSHA204 without software modifications. With the appropriate software updates, the ATSHA204 can implement all the functions of an AT8810HS Host device and continue to properly communicate with Client AT88SA102S devices.

For compatibility with the AT88SA102S, the following values should be written to the memory of the ATSHA204:

1. During configuration, OTPmode should be set to Legacy to hide the values of the first 64 bits of the OTP section, which contain a secret in the Atmel AT88SA102S.
2. The same secret and status information that would have been written to the first 88 fuse bits of the Atmel AT88SA102S should be written to the first 88 bits of the OTP section on the Atmel ATSHA204.
3. OTP bits 88 through 127 should be written with copies of the values stored in SN[4:8] within the configuration section of the Atmel ATSHA204 device. The Read command on legacy systems will always use the values in the OTP section while the Atmel ATSHA204 always uses the values in the Configuration zone during the computation of cryptographic results.
4. The key slot identified by the least significant four bits of the Atmel AT88SA102S SlotID assigned to a particular customer should be loaded with the Atmel provided value for that key.
5. The SlotConfig bits for the key slot identified in Step 4. should be set to: CheckOnly=0, SingleUse=0, EncryptRead=0, IsSecret=1, WriteConfig=1000.

The following compatibility exceptions apply:

- Those Atmel AT88SA102S systems using the BurnFuse command on the Client device cannot be replaced with the Atmel ATSHA204, as the corresponding command is not available on the ATSHA204. The same capability is implemented with the Write command, but system software modifications are necessary.
- Those Atmel AT88SA102S systems in which the system software reads and depends on a fixed value for the device revision number (RevNum at ROM address one) will find a different value in the ATSHA204.

  Note: This value is not guaranteed to be identical for all Atmel AT88SA102S devices.
- Systems including multiple Atmel AT88SA102S and/or Atmel AT88SA10HS devices on a shared single-wire bus cannot be replaced with the ATSHA204, as the Pause command operates differently.
- The key diversification strategy implemented by the ATSHA204 (when operating as a Host) is different from the similar strategy used by the Atmel AT88SA10HS. The ATSHA204 can be used as a Host authentication device for ATSHA204 Clients that include diversified keys, but those Clients will not work interchangeably with Atmel AT88SA102S Clients.
- Because of the difference in the nonvolatile memory technology and size, the secure personalization mechanism is different on the ATSHA204 as compared to the Atmel AT88SA10HS and Atmel AT88SA102S. Users will need to modify their manufacturing processes and procedures accordingly.
- The ATSHA204 cannot replace a Client Atmel AT88SA100S device used for batteries and other self-powered systems.