SAM9X60 Device Silicon Errata and Data Sheet Clarifications

SAM9X60 Device

Product Page Links

Scope

The SAM9X60 Series device that you have received conforms functionally to the current SAM9X60 data sheet (DS60001579), except for the anomalies described in this document.

The silicon issues discussed in the following pages are for silicon revisions with the device revision and device identification listed in the following table. The silicon issues are summarized in Silicon Issue Summary.

Data Sheet clarifications and corrections (if applicable) are located in Data Sheet Clarifications.

The silicon device revisions and device IDs are shown in the following table.

Table 1. SAM9X60 Device Identification

Ordering Code	Device Revision	Device Identification
		DBGU_CIDR[31:0]
SAM9X60(T)-V	A1	0x819B35A1
	A2	0x819B35A2

Note: Refer to the “Debug Unit (DBGU)” and “Product Identification System” sections in the current device data sheet for detailed information on chip identification for your specific device.

1. Silicon Issue Summary

In this table and in subsequent sections, the following applies:

- "X" means the device revision is affected by the erratum.
- "–" means the device revision is not affected by the erratum.

Table 1-1. Silicon Issue Summary

Module	Erratum	Affected Device Revisions	
		A1	A2
ROM Code	Secure Boot Mode: AES-RSA X.509 Certificate Serial Number Length Limit	X	X
	Card Detect on SDMMC not functional	X	X
	Boot failure on e.MMC memories	X	X
System Controller	System Controller Write Protection Status Register (SYSC_WPSR) Limitation	X	X
RSTC	RSTC_SR.RSTTYP not showing GENERAL_RST	X	X
OTPC	OTPC Limited Number of Packets	X	X
	OTPC Restricted Operating Range in Write Mode	X	X
	OTPC Wrong Default Configuration	X	X
PMC	ULP1 Mode Entry Procedure	X	X
SMC	Register Write Protection Not Effective on SMC_OCMS Register	X	X
AES	SPLIP mode does not work with some header sizes	X	X
FLEXCOM	FLEXCOM Sniffer Mode	X	X

2. ROM Code

2.1. Secure Boot Mode: AES-RSA X.509 Certificate Serial Number Length Limit

According to the standard RFC 5280 "Internet X.509 Public Key Infrastructure Certificate" section 4.1.2.2, the maximum length for serial numbers in X.509 certificates is 20 bytes.

When parsing the certificate chain in AES-RSA Secure Boot mode, the maximum serial number length allowed by the ROM code is 16 bytes.

Work Around

To use AES-RSA Secure Boot mode, do not use X.509 certificates with a serial number length higher than 16 bytes.

Affected Device Revisions

A1	A2						
X	X						

2.2. Card Detect on SDMMC not functional

The Card Detect feature in the SDMMC memory interface in the Boot Configuration Packet is not functional.

If an SDMMC interface is selected as the boot media, the Card Detect pin the user may have indicated in the options is not taken into account. The ROM code looks for a valid bootstrap even if the Card Detect pin is high (no card inserted).

Work Around

None

Affected Device Revisions

A1	A2						
X	X						

2.3. Boot failure on e.MMC memories

The device fails to load a bootstrap program (boot.bin) from an e.MMC **USER** partition.

Work Around

- Always use the e.MMC **BOOT** partition to store the boot.bin file and enable the e.MMC **BOOT** partition feature, and
- Set the selected SDMMCx interface as boot media 1 and boot media 2 in the Boot Configuration Packet.

Affected Device Revisions

A1	A2						
X	X						

3. System Controller Write Protection (SYSCWP)

3.1. System Controller Write Protection Status Register (SYSC_WPSR) Limitation

The status register SYSC_WPSR does not set the write access violation status flag for write-protected registers of RTC, RTT and WDT peripherals when the bit WPEN is set in SYSC_WPMR for these peripherals. However, the write protection mechanism is active.

Work Around

None

Affected Device Revisions

A1	A2						
X	X						

4. Reset Controller (RSTC)

4.1. RSTC_SR.RSTTYP not showing GENERAL_RST

In the Status register (RSTC_SR), the RSTTYP field shows BACKUP_RST instead of GENERAL_RST.

Work Around

None

Affected Device Revisions

A1	A2						
X	X						

5. OTP Controller (OTPC)

5.1. OTPC Limited Number of Packets

The number of OTP packets allowed to be written in the user area, in addition to those necessary to configure the ROM code boot features, is limited to 2. The maximum size of the payload for each packet is 8192 bits.

Work Around

None

Affected Device Revisions

A1	A2						
X	X						

5.2. OTPC Restricted Operating Range in Write Mode

The write operations in the OTPC cannot be performed over the full temperature and VDDANA power supply ranges specified.

Work Around

The write operations in the OTPC are restricted to the following ambient temperature and VDDANA power supply ranges:

- T_A = [0°C to 50°C]
- VDDANA = [3.15V to 3.45V]

Affected Device Revisions

A1	A2						
X	X						

5.3. OTPC Wrong Default Configuration

The default configuration of the OTPC cannot be used to access the OTP memory in Write mode.

Work Around

Prior to any write operation in the OTPC, the OTPC must be configured using the following code. This operation needs to be performed only once before the first write operation and whenever the peripheral reset (signal periph_nreset) is asserted.

```
#define ARRAY_SIZE(a) (sizeof(a) / sizeof((a)[0]))

/*
* writing one word lasts 350us
* the timeout was chosen to be enough for writing 10 words  **/
#define TIMEOUT 500000
#define OTPC_0    (0x1u << 0)
#define OTPC_1    16
#define OTPC_2    (0xffffu << OTPC_1)
#define OTPC_3    (0x4391u << OTPC_1)

static void otp_sam9x60_fixup(void)
{
       static const uint32_t fixup0[4] = {0x04194801, 0x01000000, 0x00000008, 0x00000000};
       static const uint32_t fixup1[4] = {0xfb164801, 0x4c017d12, 0x02120e01, 0x00004000};
       __IO uint32_t *OTPC_4   = (__IO uint32_t *)((uint8_t *)OTPC + 0x090);
       __IO uint32_t *OTPC_5 = (__IO uint32_t *)((uint8_t *)OTPC + 0x0A0);
       __IO uint32_t *OTPC_6 = (__IO uint32_t *)((uint8_t *)OTPC + 0x0B0);
       uint32_t timeout;
       int i;

       timeout = TIMEOUT;
       *OTPC_4 = OTPC_0 | OTPC_3;
```

```
        while (!(OTPC->OTPC_SR & OTPC_SR_UNLOCK) && --timeout > 0);

        for (i = 0; i < ARRAY_SIZE(fixup0); i++)
               OTPC_5[i] = fixup0[i];

        for (i = 0; i < ARRAY_SIZE(fixup1); i++)
               OTPC_6[i] = fixup1[i];

        timeout = TIMEOUT;
        *OTPC_4 = OTPC_3;
        while ((OTPC->OTPC_SR & OTPC_SR_UNLOCK) && --timeout > 0); }
```

Affected Device Revisions

A1	A2						
X	X						

6. Power Management Controller (PMC)

6.1. ULP1 Mode Entry Procedure

If one or more read or write accesses to the PMC user interface follow the last instruction to enter ULP1 mode (set CKGR_MOR.ULP1), the ULP1 mode may be exited immediately after the entry.

Work Around

Add two dummy read accesses outside of the PMC user interface just after setting the CKGR_MOR.ULP1 bit.

Affected Device Revisions

A1	A2						
X	X						

7. Static Memory Controller (SMC)

7.1. Register write protection not effective on SMC_OCMS register

The register SMC_OCMS is not write-protected when the bit WPEN is set in SMC_WPMR.

Work Around

None

Affected Device Revisions

A1	A2						
X	X						

8. Advanced Encryption Standard (AES)

8.1. SPLIP mode does not work with some header sizes

The Secure Protocol Layers Improved Performances (SPLIP) mode does not work when the ESP header is not an integer multiple of 4 words.

Work Around

When the ESP header is not an integer multiple of 4 words, disable SPLIP mode to stop AES from automatically uploading the encrypted payload into SHA, and use the central DMA to feed SHA with the encrypted payload.

Affected Device Revisions

A1	A2						
X	X						

9. Flexible Serial Communication Controller (FLEXCOM)

9.1. FLEXCOM Sniffer Mode

When using FLEXCOM in Sniffer mode, the peripheral TWI*n+1* cannot be configured to analyze the peripheral TWI*n* (n being the instance index of the TWI) in a full transparent mode via predefined internal connections between TWI instances.

Work Around

Configure TWI*n* to analyze TWI*n+1*.
Note: When n=12 (FLEXCOM12), n+1 means 0 (FLEXCOM0).

Affected Device Revisions

A1	A2						
X	X						

10. Data Sheet Clarifications

There are no known data sheet clarifications as of this publication date.

11. Revision History

11.1. DS80000846G - 06/2025

Added Boot failure on e.MMC memories

11.2. DS80000846F - 01/2025

Throughout: • “Silicon revision A0” now referred to as “Device revision A2” • “Silicon revision A1” now referred to as “Device revision A1”
Added: • Card Detect on SDMMC not functional • RSTC_SR.RSTTYP not showing GENERAL_RST • SPLIP mode does not work with some header sizes
Data Sheet Clarifications: removed “OTPC Dependency to Main RC Oscillator” issue

11.3. DS80000846E - 10/2021

Added silicon revision information throughout

11.4. DS80000846D - 09/2021

Updated SAM9X60 Silicon Device Identification table with additional chip ID
Added OTPC Dependency to Main RC Oscillator in Data Sheet Clarifications

11.5. DS80000846C - 09/2020

Updated OTPC Limited Number of Packets
Added Secure Boot Mode: AES-RSA X.509 Certificate Serial Number Length Limit

11.6. DS80000846B - 02/2020

Added Flexible Serial Communication Controller (FLEXCOM)
Data Sheet Clarifications: removed "EBI Controls in Special Function Registers (SFR)"

11.7. DS80000846A - 10/2019

First issue.

Microchip Information

Trademarks

The “Microchip” name and logo, the “M” logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries (“Microchip Trademarks”). Information regarding Microchip Trademarks can be found at https://www.microchip.com/en-us/about/legal-information/microchip-trademarks.

ISBN: 979-8-3371-1243-5

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP “AS IS”. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP’S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip products are strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Product Page Links

SAM9X60