

## Product Development Software Release Form

The software item documented in this form is the property of Intersil Americas Inc. Transmittal, receipt, or possession of this document does not express, license, or imply any rights to use, sell, design, or manufacture from this information or the software documented herein. No reproduction, publication, or disclosure of this information, in whole or in part, shall be made without prior written authorization from an authorized representative of Intersil Americas Inc.

**NOTE: THIS DOCUMENT CONTAINS SENSITIVE INFORMATION AND HAS RESTRICTED DISTRIBUTION.**

**Product:** 3842 PCMCIA/PCI Secondary Firmware  
**Version:** 1.4.9  
**Classification:** Firmware  
**Intended Distribution:** Premier Distribution  
**Date Submitted:** 09 May 2002  
**Submitted By:** PRISM® Quality Engineering

### Description:

The **3842 PCMCIA/PCI Secondary Firmware** provides 802.11 Station functionality for HFA3842-based PCMCIA or PCI 802.11 NICs.

### Purpose:

This release corrects an error that caused receptions to be blocked when running with Windows XP zero-config enabled.

### System Environment:

3842 PCMCIA/PCI Primary Firmware with supplier interface compatibility range of [4-4]

### Hardware Supported:

3842 Evaluation Board (0x800A)

AMD parallel flash: PRISM® II PCMCIA (0x800B), PRISM II Mini-PCI (0x8012), PCI-bridge (0x8016), PRISM III PCMCIA (0x801A), PRISM III Mini-PCI (0x8021)

SST parallel flash: PRISM II PCMCIA (0x800C), PRISM II Mini-PCI (0x8013), PCI-bridge (0x8017), PRISM III PCMCIA (0x801B), PRISM III Mini-PCI (0x8022)

AT45DB011 compatible large serial flash: PRISM II PCMCIA (0x800D), PRISM II Mini-PCI (0x8014), PCI-bridge (0x8018), PRISM III PCMCIA (0x801C), PRISM III Mini-PCI (0x8023)  
*[NOTE: Large serial is not recommended for new reference designs.]*

AT24C08 compatible small serial flash: PRISM II PCMCIA (0x800E), PRISM II Mini-PCI (0x8015), PCI-bridge (0x8019), PRISM III PCMCIA (0x801D), PRISM III Mini-PCI (0x8024)

### Files Released:

SF010409.HEX      Motorola S-Record File (Secondary Firmware) for 800A, 800B, 800C, 800D, 8012, 8013, 8014, 8016, 8017, 8018, 801A, 801B, 801C, 8021, 8022, 8023

RF010409.HEX      Motorola S-Record File (RAM-download Secondary Firmware) for 800A, 800B, 800C, 800D, 800E, 8012, 8013, 8014, 8015, 8016, 8017, 8018, 8019, 801A, 801B, 801C, 801D, 8021, 8022, 8023, 8024

SEC42RFM.PDF      3842 PCMCIA Secondary Firmware release form

## Installation Instructions:

The **3842 PCMCIA Secondary Firmware** is installed on a target platform with the Flash utility. A 3842 PCMCIA Primary Firmware image must be installed before the Secondary image can be installed.

## Limitations:

Known bugs or features not implemented are:

1. 802.11 WEP Key mapping not implemented.
2. 802.11 compliant CCA not implemented.
3. Frames are not fragmented in HostAP mode.
4. Current Power State RIDs may report incorrect values. (TI #45)
5. SIFS timings are often too long. (TI #90)
6. The 'logical collision detection' mechanism sometimes causes the retry bit to be incorrectly set on the first transmission of a frame. (TI #92)
7. The auto state of setting longPreamble and shortPreamble in the Configuration Record cnfPreamble is not supported. Short Preambles are transmitted when bit 1 of cnfPreamble is set to 1 and long preambles are transmitted when bit 1 is set to 0. (TI #101)

## Release History:

**\*\* 01.04.09 – 26 Apr 2002 \*\***

1. This release has the label 'S42V01.04.09' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.4.9 when the Secondary Functions firmware ID RID (RID FD20) is queried. The build sequence number is 0.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. The required primary supplier interface compatibility range remains [4-4].
5. Corrected diagnostic scanning to skip powering on the radio before starting a scan if the radio was already powered up. Previously, the unnecessary power on could start at a point that could cause the firmware to hang if power save was enabled (FB#398). An initialization routine was modified to always invoke a receive cleanup routine to ensure that the receive state machine was in an idle state.

**\*\* 01.04.08 – 10 Apr 2002 \*\***

1. This release has the label 'S42V01.04.08' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.4.8 when the Secondary Functions firmware ID RID (RID FD20) is queried. The build sequence number is 0.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Fixed a bug in the RAM download 1.4.7 image that caused erratic behavior from the download command 0x322 most noticeably on serial flash platforms.

**\*\* 01.04.07 – 28 Mar 2002 \*\***

1. This release has the label 'S42V01.04.07' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.4.7 when the Secondary Functions firmware ID RID (RID FD20) is queried. The build sequence number is 0.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Corrected an error that caused an association failure when a zero configuration scan was initiated during the association process (FB#371).

**\*\* 01.04.06 – 26 Mar 2002 \*\***

1. This release has the label 'S42V01.04.06' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.4.6 when the Secondary Functions firmware ID RID (RID FD20) is queried. The build sequence number is 0.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Corrected an error that prevented rescans from working.
5. Version 01.03.02 introduced the filtering of weak WEP IVs of the form xxFFyy. Weak IVs of this type are not generated.

**\*\* 01.04.05 – 21 Mar 2002 \*\***

1. This release has the label 'S42V01.04.05' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.4.5 when the Secondary Functions firmware ID RID (RID FD20) is queried. The build sequence number is 0.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Corrected an error that could cause the scanning process to enter a stalled state.
5. Corrected an error that could cause the driver to no longer be able to communicate with the firmware.
6. A modification was made to bypass an error that prevented a primary from being able to perform a flash download if a RAM based secondary was running. There is a caveat; however, a secondary image must exist in the flash.
7. Version 1.4.4 was skipped in order to provide a common secondary version of 1.4.5 across all platforms.

**\*\* 01.04.03 – 11 Mar 2002 \*\***

1. This release has the label 'S42V01.04.03' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.4.3 when the Secondary Functions firmware ID RID (RID FD20) is queried. The build sequence number is 0.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Scanning for a non-existent access point should no longer cause a firmware lock up (FB#361).
5. The first WEP frame generated by the firmware after initialization is now sent without error (FB#362).
6. A diagnostic scan now correctly transmits probe requests on the first selected channel (FB#364).

7. IBSS stations will now report the lowest possible signal, silence, and communication quality levels when searching for an IBSS.
8. Corrected a problem that allowed an IBSS station to operate on a channel adjacent to the correct channel.
9. Corrected an error that caused an IBSS station to stop functioning after a host scan request.
10. Removed a RAM test diagnostic routine that put the firmware into an infinite loop as part of the diagnose command.
11. Corrected an error that prevented probe requests from being passed to the host when operating in host based access point mode.

**\*\* 01.04.02 – 25 Feb 2002 \*\***

1. This release has the label 'S42V01.04.02' applied on the source tree under Performce.
2. Reports a major/minor/variant version of 1.4.2 when the Secondary Functions firmware ID RID (RID FD20) is queried. The build sequence number is 0.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Corrected an error in the re-association process (FB#357).

**\*\* 01.04.01 – 11 Feb 2002 \*\***

1. This release has the label 'S42V1.4.1' applied on the source tree under Performce.
2. Reports a major/minor/variant version of 1.4.1 when the Secondary Functions firmware ID RID (RID FD20) is queried. The build sequence number is 0.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Corrected RxRate value in the linktest response frame introduced in the last release.

**\*\* 01.04.00 – 8 Feb 2002 \*\***

1. This release has the label 'S42V1.4.0' applied on the source tree under Performce.
2. Reports a major/minor/variant version of 1.4.0 when the Secondary Functions firmware ID RID (RID FD20) is queried. The build sequence number is 0.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Fixed a scanning hang problem seen under Windows XP (FB#331).
5. Corrected RxSignal and RxNoise values in linktest response frames.
6. Fixed a problem in Communication Tallies information frame when 32 bit tallies were enabled.
7. Corrected a problem that caused the capability field in beacons to never indicate support for short preambles.
8. Corrected a problem that caused intermittent failures resulting in a loss of communication with the driver (FB#344).
9. Fixed a hang condition seen on certain hardware designs when using firmware WEP.
10. Added code to ignore beacons from an AP that abruptly changes its channel ID.

**\*\* 1.3.7 – 15 Jan 2002 \*\***

1. This release has the label 'S42V1.3.7' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.3.7 when the Secondary Functions firmware ID RID (RID FD20) is queried. The build sequence number is 0.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Build sequence numbers are now 0-127 for releases and 128+ for developer builds.
5. Adds support for PRISM III.
6. Pseudo IBSS mode was changed to stop sending a disconnect info event upon disabling.
7. Made changes to reduce power consumption in the states following initialization and disable (FB#273).
8. Corrected a problem during PowerSave that allowed a station to go to sleep between frames even though the station was actively receiving data (such as during a set of fragments for a data frame), thereby adversely affecting throughput performance.
9. JoinRequest RID was not turning the radio on to re-associate with an AP (FB#325).
10. Host Roaming Mode 2 was causing subsequent scans to scan incorrect channels (FB#324).
11. Fixed a problem where a station could lose the connection with the AP while operating in PowerSave.
12. Added code for handling heavy traffic conditions.
13. Fixed a bug that could result in using incorrect rates in IBSS mode when 2 or more stations are participating.

**\*\* 1.3.6 – 1 Nov 2001 \*\***

1. This release has the label 'S42V1.3.6' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.3.6 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Adjusted channel change delays to allow proper operation on PRISM 3. This change is compatible with PRISM II and affects 3861 and newer baseband processors.
5. Modified firmware to prevent beacons and probe responses from being transmitted if a scan is in progress in an IBSS configuration. This fixes a hang condition that could affect Windows-XP™ "zero configuration".
6. Adjusted Rate fallback values and made the fallback algorithm less aggressive in order to help throughput.
7. Corrected the IBSS beacon timestamp value, which could cause other IBSS stations to calculate their timestamp as always greater, in which case, stations would then not adopt elements in the beacon.

**\*\* 1.3.5 – 5 Oct 2001 \*\***

1. This release has the label 'S42V1.3.5' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.3.5 when the Secondary Functions firmware ID RID (RID FD20) is queried.

3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. IBSS functionality has been reverted to its functional 1.3.2 level.
5. An error that could cause the firmware to hang when scanning has been corrected (FB#242).
6. Buffer allocation has been modified to provide more fairness between buffers allocated for reception and transmission.
7. Changes were made to prevent erroneous data from being transferred over the PCI bus.

A primary plug record (408) defines the number of milliseconds to delay going idle after the host has set up a buffer access path. The default is 100ms; the minimum is zero; the maximum is 65,535. This record and the associated code was added to prevent data corruption that can occur over the PCI bus if an access is made when the chip is in an idle state.

Control Store writes are now always enabled. This change was made to prevent data corruption that can occur over the PCI bus if an access is made when the chip is executing from on-chip control store.

**\*\* 1.3.4 – 21 Sep 2001 \*\***

1. This release has the label 'S42V1.3.4' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.3.4 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Fixes a stall condition that would inhibit frame transmits for up to a few seconds.
5. Fixes a common stall condition in IBSS mode that would last up to one beacon interval.

**\*\* 1.3.3 – 17 Sep 2001 \*\***

1. This release has the label 'S42V1.3.3' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.3.3 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-9].
4. Added an API to support the AutoUnknown mode with createIBSS (RID FC81). When used with cnfPortType (FC00), the host can configure the NIC to attempt to join an ESS and in the absence of one, create an IBSS:

Connection Type	cnfPortType	createIBSS
Ndis802_11IBSS	0	0
Ndis802_11Infrastructure	1	NA
Ndis802_11AutoUnknown	0	1

Word Offset	Field name	Size (words)
0	RecordLen: 2	1
1	RID: FC81	1
2	IBSSFlags	1

***Field descriptions:***

Name: IBSSFlags

Description: This value identifies the WEP key ID to disable.

00b = Join/create IBSS

01b = Join ESS or join/create IBSS

10b = Join IBSS only (do not create)

11b = Join ESS or IBSS (do not create an IBSS)

Format: bit-map

Values: default: 0

5. Corrected a rare conflict between a TSF update request and a transmit command (TI#241). This conflict was causing the firmware to hang when WEP was enabled.
6. Corrected a conflict between roaming and the Host Scan feature (initiated by FCE5). This was causing improper operation under Windows XP.
7. Corrected a condition where a flood of authentication frames would be transmitted in rapid succession when failing to associate with an AP.
8. Changed the maximum value for signal level (reported by FD43) from 139 to 154 to match our documentation.
9. Corrected the frame control word that is passed to the host when in Monitor Mode and Host Decrypt is enabled (TI#226).

**\*\* 1.3.2 – 17 Aug 2001 \*\***

1. This release has the label 'S42V1.3.2' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.3.2 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-8]
4. Added an additional RID FD8A (get authentication algorithm used) for NDIS5.1.
5. Corrected an error that caused infrequent encryption failures.
6. Corrected an error that caused a transmitter stall after the reception of an invalid control frame.
7. Corrected an error that caused stations to report poor link quality when the beacon interval was small <40ms (TI233).

**\*\* 1.3.1 – 9 Aug 2001 \*\***

1. This release has the label 'S42V1.3.1' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.3.1 when the Secondary Functions firmware ID RID (RID FD20) is queried.

3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-7].
4. Corrected a problem that caused PSPoll frames to have an incorrect PLCP header.

**\*\* 1.3.0 – 6 Aug 2001 \*\***

1. This release has the label 'S42V1.3.0' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.3.0 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-7].
4. Added NDIS5.1 HostScan feature, RIDs FD89 (get HSRT), FCE5 (initiate host scan), FCB6 (WEP Key Status), and F103 (HSRT info frame).
5. IBSS will now select an NCB to reuse when table is full (TI#200).
6. Fixed an AP out of range scanning problem (TI#227). Corrected a number of problems related to roaming while power saving was enabled.
7. Added an enhanced retry fallback mechanism (RID FCB5).

**\*\* 1.2.0 – 6 Jul 2001 \*\***

1. This release has the label 'S42V1.2.0' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.2.0 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-6].
4. Modified the data returned by FD43 so tools will more accurately display signal quality.
5. Reduced the cell search threshold for low density, and revised the thresholds for medium and high-density settings.
6. Comms quality RID, FD51, now passes up dBm values as signed 16-bit values.
7. Changed the way signal level is averaged so that missing beacons will not pull down signal quality as quickly. This helps to keep 3863 platforms connected with some 3861 APs.
8. Corrected the TIM generation in Beacons.
9. Added transmission of a Deauthenticate frame following a Disable command. (TI #88)
10. Corrected the ReadTIMCtrl RID function, FC40, which would read the wrong word from the table if the given byte address was an odd value.
11. Added code to support a deeper level of power savings.
12. Enhanced power savings mode replaces the original power savings mode.
13. MKK filtering for channel 14 is now supported.
14. The MAC will now go idle when no events are present and unmasked.
15. Corrected an error that could cause false ICV failures.
16. Corrected an error that could generate a false, logical medium busy indication.
17. Changed transmit control timings to meet Interface Control Document specifications.
18. Fixed duration values in fragmented frames.

**\*\* 1.1.1 – 31 May 2001 \*\***

1. This release has the label 'S42V1.1.1\_Label' applied on the source tree under Perforce.



2. Reports a major/minor/variant version of 1.1.1 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-6].
4. Improved infrastructure operation in weak signal conditions by changing the way our communications quality metric is calculated and effectively reducing the threshold at which we report a loss of service to the host.

**\*\* 1.1.0 – 10 Apr 2001 \*\***

1. This release has the label 'S42V1.1.0' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.1.0 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-6].
4. Corrected a problem in PowerSave firmware that caused lockups and poor performance (TI #188).

**\*\* 1.0.2 – 20 Mar 2001 \*\***

1. This release has the label 'S42V1.0.2' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.0.2 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-6].
4. Added support for 128-bit WEP.
5. Corrected a problem that caused zero length data frames to be incorrectly identified as 802.11h or RFC1042 frames. (TI #120)

**\*\* 1.0.1 – 28 Feb 2001 \*\***

1. This release has the label 'S42V1.0.1' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.0.1 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-6].
4. Corrected buffer count masking bug that could result in corrupted broadcast frames (TI #161).
5. Fixed bug where the JoinRequest action RID (FCE2) would hang the card if the SSID specified is blank (TI#150).
6. Fixed 802.11 Power Save mode (TI #145).

**\*\* 1.0.0 – 7 Feb 2001 \*\***

1. This release has the label 'S42V1.0.0' applied on the source tree under Perforce.
2. Reports a major/minor/variant version of 1.0.0 when the Secondary Functions firmware ID RID (RID FD20) is queried.
3. Secondary supplier compatibility range (RID FD21) has a bottom to top range of [1-6].