発行日：2024年9月9日

RENESAS TECHNICAL UPDATE

〒135-0061 東京都江東区豊洲 3-2-24 豊洲フォレシア
ルネサス エレクトロニクス株式会社

製品分類	MPU ＆MCU		発行番号	TN-RA*-A0118A/J	Rev.	第1版
題名	RA8M1 グループ、RA8D1 グループ、RA8T1 グループ、セキュリティ機能記述に関する修正		情報分類	技術情報		
適用製品	RA8M1 グループ RA8D1 グループ RA8T1 グループ	対象ロット等 すべて	関連資料	RA8M1 グループ ユーザーズマニュアル ハードウェア編 Rev1.10 RA8D1 グループ ユーザーズマニュアル ハードウェア編 Rev1.10 RA8T1 グループ ユーザーズマニュアル ハードウェア編 Rev1.10 アプリケーションノート Renesas Boot Firmware for RA8M1 MCU Group Rev. 1.10 Renesas Boot Firmware for RA8D1 MCU Group Rev. 1.10 Renesas Boot Firmware for RA8T1 MCU Group Rev. 1.10		

セキュリティ機能に関する記述について修正が入ります。

【ユーザーズマニュアル ハードウェア編に対しての修正】

43.6 セキュアファクトリプログラミング（RA8M1、RA8D1 用）
37.5 セキュアファクトリプログラミング（RA8T1 用）

修正前

非セキュア環境でのセキュアファクトリプログラミングをさらにサポートするために、DLM ステート、保護レベル、および認証キーを一つのブートファームウェアコマンドで全て設定できます。このブートファームウェアコマンドに関して以下の点に注意してください。

- 暗号化ファームウェアプログラミングは、MCU が OEM 状態のときのみ実行できます。
- このコマンドは MCU の保護レベルを変更してしまいます。初期 PL は PL2 でなければなりません。最終 PLは PL0 でなければなりません。
- DLM ステートが OEM 状態のままになりそうな場合、AL2 キーをインジェクトする必要があります。オプションで AL1 キーもインジェクト可能です。
- MCU は LCK_BOOT 状態に遷移できます。この場合、AL キーはインジェクトできません。
- AL キーはイメージ暗号化キーと同じ UFPK でラッピングする必要があります。
- このコマンドは、暗号化されたファームウェアイメージをプログラムする前に、オプション設定メモリを除くすべてのコードおよびデータフラッシュエリアを消去します。永久ロックブロックがある場合、このコマンドは実行できません。
- 現在のレジスタ設定またはスタートアップ領域選択およびスタートアップバンク選択に関連するレジスタへの書き込み値が下記以外の場合、このコマンドは実行されません。
  - SAS.BTFLG = 1b

- BANKSEL.BANKSWP[2:0] = 111b
- BANKSEL_SEC.BANKSWP[2:0] = 111b

- 暗号化されたファームウェアイメージには、デフォルト値で使用しない設定を含めた全てのオプション設定メモリ値を含める必要があります。ただし、以下の領域が書き込み保護されている場合、これらの領域の書き込みデータはイメージに含めないでください。イメージに含まれていると、このコマンドがエラー終了することになります。
  - SAS レジスタ
  - データフラッシュオプション設定メモリ内のロック可能領域 0～2

修正後

非セキュア環境でのセキュアファクトリプログラミングをさらにサポートするために、DLM ステート、保護レベル、および認証キーを一つのブートファームウェアコマンドで全て設定できます。このブートファームウェアコマンドに関して以下の点に注意してください。

- 暗号化ファームウェアプログラミングは、MCU が OEM 状態のときのみ実行できます。
- このコマンドは MCU の保護レベルを変更してしまいます。初期 PL は PL2 でなければなりません。最終 PLは PL0 でなければなりません。
- DLM ステートが OEM 状態のままになりそうな場合、AL2 キーをインジェクトする必要があります。AL1 キーはインジェクトしないでください。
- MCU は LCK_BOOT 状態に遷移できます。この場合、AL キーはインジェクトできません。
- AL2 キーはイメージ暗号化キーと同じ UFPK でラッピングする必要があります。
- このコマンドは、暗号化されたファームウェアイメージをプログラムする前に、オプション設定メモリを除くすべてのコードおよびデータフラッシュエリアを消去します。永久ロックブロックがある場合、このコマンドは実行できません。
- 現在のレジスタ設定またはスタートアップ領域選択およびスタートアップバンク選択に関連するレジスタへの書き込み値が下記以外の場合、このコマンドは実行されません。
  - SAS.BTFLG = 1b
  - BANKSEL.BANKSWP[2:0] = 111b
  - BANKSEL_SEC.BANKSWP[2:0] = 111b
- 暗号化されたファームウェアイメージには、デフォルト値で使用しない設定を含めた全てのオプション設定メモリ値を含める必要があります。ただし、以下の領域が書き込み保護されている場合、これらの領域の書き込みデータはイメージに含めないでください。イメージに含まれていると、このコマンドがエラー終了することになります。
  - SAS レジスタ
  - データフラッシュオプション設定メモリ内のロック可能領域 0～2

【アプリケーションノート Renesas Boot Firmware for RA8M1/RA8D1/RA8T1 に対しての修正】

修正前

6.33.2.2 Data Packet [Parameter]

<table>
<tr><td>SOD</td><td>(1 byte)</td><td>81h</td></tr>
<tr><td>LNH</td><td>(1 byte)</td><td>00h</td></tr>
<tr><td>LNL</td><td>(1 byte)</td><td>2Dh</td></tr>
<tr><td>RES</td><td>(1 byte)</td><td>1Ah (OK)</td></tr>
<tr><td>NCE</td><td>(12byte)</td><td>Nonce used for encrypting parameters.
Nonce length is 12 bytes and counter length is 4 bytes.</td></tr>
<tr><td>PRM</td><td>(16 bytes)</td><td>Encrypted parameters.
Encryption method is AES128-CCM mode (NIST SP800-38C).
Data format before encryption:
<table>
<tr><th>1st–4th bytes</th><th>5th byte</th><th>6th–8th bytes</th></tr>
<tr><td>LOD</td><td>TRN</td><td>(reserved: FFh)</td></tr>
<tr><th colspan="3">9th–16th bytes</th></tr>
<tr><td colspan="3">(reserved: FFh)</td></tr>
</table>
Parameter details:
<table>
<tr><td>LOD (4 bytes)</td><td>Total length of "encrypted user data and write address/size""
• Must be greater than 0/
• Must be multiple of encryption block size (16 bytes for AES128)
For example:
LOD = 00104000h = 00h, 10h, 40h, 00h when:
• Total length of raw image=1MB=100000h
• Length of SAD, SIZE and reserved=4000h(*)
*) 16 bytes per packet as described below</td></tr>
<tr><td>TRN (1 byte)</td><td>Transition pattern:
• 00h: PL0 with AL2_key and AL1_key
• 01h: PL0 with AL2_key
• 02h: LCK_BOOT</td></tr>
</table>
</td></tr>
<tr><td>MAC</td><td>(16 bytes)</td><td>MAC for Encrypted parameters</td></tr>
<tr><td>SUM</td><td>(1 byte)</td><td>Sum data</td></tr>
<tr><td>ETX</td><td>(1 byte)</td><td>03h</td></tr>
</table>

修正後

6.33.2.2 Data Packet [Parameter]

<table>
<tr><td>SOD</td><td>(1 byte)</td><td>81h</td></tr>
<tr><td>LNH</td><td>(1 byte)</td><td>00h</td></tr>
<tr><td>LNL</td><td>(1 byte)</td><td>2Dh</td></tr>
<tr><td>RES</td><td>(1 byte)</td><td>1Ah (OK)</td></tr>
<tr><td>NCE</td><td>(12byte)</td><td>Nonce used for encrypting parameters.
Nonce length is 12 bytes and counter length is 4 bytes.</td></tr>
<tr><td>PRM</td><td>(16 bytes)</td><td>Encrypted parameters.
Encryption method is AES128-CCM mode (NIST SP800-38C).
Data format before encryption:
<table>
<tr><th>1st–4th bytes</th><th>5th byte</th><th>6th–8th bytes</th></tr>
<tr><td>LOD</td><td>TRN</td><td>(reserved: FFh)</td></tr>
<tr><th colspan="3">9th–16th bytes</th></tr>
<tr><td colspan="3">(reserved: FFh)</td></tr>
</table>
Parameter details:
<table>
<tr><td>LOD (4 bytes)</td><td>Total length of "encrypted user data and write address/size""
• Must be greater than 0/
• Must be multiple of encryption block size (16 bytes for AES128)
For example:
LOD = 00104000h = 00h, 10h, 40h, 00h when:
• Total length of raw image=1MB=100000h
• Length of SAD, SIZE and reserved=4000h(*)
*) 16 bytes per packet as described below</td></tr>
<tr><td>TRN (1 byte)</td><td>Transition pattern:
• 01h: PL0 with AL2_key
• 02h: LCK_BOOT</td></tr>
</table></td></tr>
<tr><td>MAC</td><td>(16 bytes)</td><td>MAC for Encrypted parameters</td></tr>
<tr><td>SUM</td><td>(1 byte)</td><td>Sum data</td></tr>
<tr><td>ETX</td><td>(1 byte)</td><td>03h</td></tr>
</table>

Security Key Management Tool V.1.07(2024 年 8 月 30 日リリース予定) で、この修正に対応いたします。

Secure Factory Programming 機能を使用する場合、V.1.07 以降をご使用ください。