UltraScale FPGA の RSA 認証およびサポートするコンフィギュレーション モード

XCN15038 (v1.0) 2015 年 12 月 21 日　　製品変更通知

概要

この通知は、ビットストリーム コンフィギュレーションに用いる RSA 認証機能が Kintex UltraScale および Virtex UltraScale FPGA の特定のコンフィギュレーション モードに限定されることをお知らせするものです。

説明

サポートされていないコンフィギュレーション モードで RSA 認証を使用したビットストリームを読み込むと、認証エラーが発生し、デバイスがロック ダウンする、または有効な場合はフォールバック コンフィギュレーション ビットストリームを読み込む可能性があります。表 1 に、コンフィギュレーション ビットストリームの RSA 認証をサポートする特定のコンフィギュレーション モードを示します。

この制限は、すべての Kintex UltraScale および Virtex UltraScale FPGA に適用されますが、以前の資料では KU025 以外は記載されていませんでした。表 1 の情報を記載するため、『UltraScale アーキテクチャ コンフィギュレーション ユーザー ガイド』(UG570) が v1.6 にアップデートされています。

表 1 : UltraScale FPGA およびコンフィギュレーション モード別の RSA 認証のサポートの有無

コンフィギュレーション インターフェイス	データ バス幅	Kintex UltraScale FPGA				Virtex UltraScale FPGA		
		KU025(3)	KU035 KU040	KU060 KU085 K U115	KU095	VU080 VU095	VU065 VU125 VU160 VU190	VU440
SelectMAP	32	N/A	あり(1)	あり(1)	あり(1)	あり(1)	あり(1)	あり(1)
	16	N/A	あり(1)	あり(1)	あり(1)	あり(1)	あり(1)	あり(1)
	8	N/A	なし	なし	あり(1)	あり(1)	なし	あり(1)
BPI	16	N/A	あり	あり(2)	あり	あり	あり	あり
	8	N/A	なし	なし	あり(2)	あり(2)	なし	あり
SPI	8	N/A	なし	なし	あり	あり	なし	あり
	4	N/A	なし	なし	なし	なし	なし	あり
	2	N/A	なし	なし	なし	なし	なし	なし
	1	N/A	なし	なし	なし	なし	なし	なし
JTAG	1	N/A	なし	なし	なし	なし	なし	なし
シリアル	1	N/A	なし	なし	なし	なし	なし	なし

注記 :
1. SelectMAP データの不連続読み込みが CSI_B 信号のディアサートによって実行される場合、サポートされません。
2. 非同期ページ読み出しが使用される場合、サポートされません。
3. Kintex UltraScale KU025 FPGA には RSA 認証のサポートがなく、この通知の対象外です。

© Copyright 2015 Xilinx, Inc. Xilinx、Xilinx のロゴ、Artix、ISE、Kintex、Spartan、UltraScale、Virtex、Vivado、Zynq、およびこの文書に含まれるその他の指定されたブランドは、米国およびその他各国のザイリンクス社の商標です。AMBA、AMBA Designer、ARM、ARM1176JZ-S、CoreSight、Cortex、および PrimeCell は EU およびその他各国の ARM 社の登録商標です。PCI、PCIe、PCI Express は PCI-SIG の商標であり、使用にはライセンスが必要です。すべてのその他の商標は、それぞれの保有者に帰属します。

該当製品

この変更は、表 1 に示す Kintex UltraScale と Virtex UltraScale FPGA の全スピード グレード、パッケージ、温度範囲のデバイスおよびそれらの SCD (Specification Control Document) デバイスに該当します。

トレーサビリティ

図 1 に示すように、該当製品は、青色の破線で囲んだ Kintex UltraScale または Virtex UltraScale ファミリ名、あるいはそれぞれに対応する KU または VU デバイス タイプから特定できます。

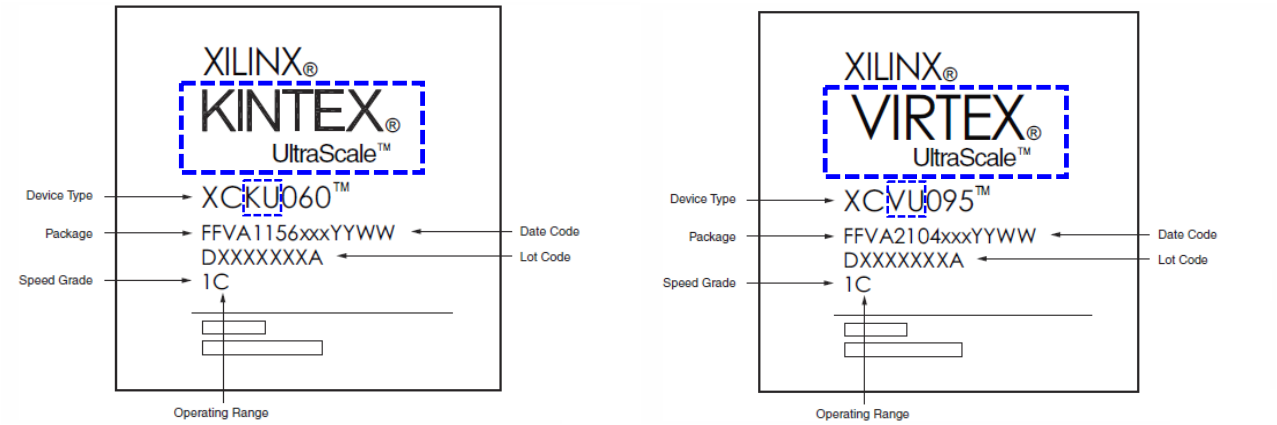

図 1 : デバイス トップ マークの例

推奨事項

ザイリンクスは、RSA 認証機能を使用するカスタマーに対して FPGA コンフィギュレーション システムおよびボード デザインを確認し、適宜対処されることをお勧めします。サポート対象のコンフィギュレーション モードと詳細は、この文書の表 1 または UG570 の表 8-1 を参照してください。

コンフィギュレーション ビットストリームの別の認証方法として、GCM (Galois/Counter Mode) アルゴリズムを用いた AES (Advanced Encryption Standard) 復号化および認証も UltraScale FPGA はサポートしています。AES-GCM 機能は、すべての Virtex UltraScale および Kintex UltraScale FPGA (KU025 FPGA を含む) の全コンフィギュレーション モードでサポートされています。セキュリティ要件に応じて、AES-GCM が最適なオプションであるかどうかを判断してください。AES-GCM は、対称キーを用いた暗号化アルゴリズム (認証を含む) で、RSA は非対称の認証アルゴリズムです。AES-GCM 暗号化を使用する場合の FPGA コンフィギュレーション機能の補足事項は、UG570 を参照してください。

お問い合わせ

この通知に対する回答は必要ありません。その他ご不明な点、ご質問等ございましたら、ザイリンクス テクニカル サポートまでお問い合わせください。

重要なお知らせ : ザイリンクス カスタマー通知 (XCN、XDN、Quality Alert) リリースのお知らせは、ザイリンクスのサポート ウェブサイト (http://japan.xilinx.com/support) から e-mail で受け取ることができます。アカウントご登録後、資料とデザイン アドバイザリ アラートにカスタマー変更通知が含まれるようにカスタマイズしてください。ザイリンクス サポート サイトでは、指定された製品に関する新規および更新情報、データシートやエラッタ、アプリケーション ノートなどに関するアラートを受け取ることができるサービスを提供しています。登録方法は、ザイリンクス アンサー 18683 (http://japan.xilinx.com/support/answers/18683.htm) を参照してください。

その他の資料

『UltraScale アーキテクチャ コンフィギュレーション ユーザー ガイド』(UG570)、v1.6 またはそれ以降 :

http://japan.xilinx.com/cgi-bin/docs/ndoc?t=user_guides;d=j_ug570-ultrascale-configuration.pdf

改訂履歴

次の表に、この文書の改訂履歴を示します。

日付	バージョン	内容
2015 年 12 月 21 日	1.0	初版

免責事項

本通知に基づいて貴殿または貴社 (本通知の被通知者が個人の場合には「貴殿」、法人その他の団体の場合には「貴社」。以下同じ) に開示される情報 (以下「本情報」といいます) は、ザイリンクスの製品を選択および使用することのためにのみ提供されます。適用される法律が許容する最大限の範囲で、(1) 本情報は「現状有姿」、および全て受領者の責任で (with all faults) という状態で提供され、ザイリンクスは、本通知をもって、明示、黙示、法定を問わず (商品性、非侵害、特定目的適合性の保証を含みますがこれらに限られません)、全ての保証および条件を負わない (否認する) ものとします。また、(2) ザイリンクスは、本情報 (貴殿または貴社による本情報の使用を含む) に関係し、起因し、関連する、いかなる種類・性質の損失または損害についても、責任を負わない (契約上、不法行為上 (過失の場合を含む)、その他のいかなる責任の法理によるかを問わない) ものとし、当該損失または損害には、直接、間接、特別、付随的、結果的な損失または損害 (第三者が起こした行為の結果被った、データ、利益、業務上の信用の損失、その他あらゆる種類の損失や損害を含みます) が含まれるものとし、それは、たとえ当該損害や損失が合理的に予見可能であったり、ザイリンクスがそれらの可能性について助言を受けていた場合であったとしても同様です。
ザイリンクスは、本情報に含まれるいかなる誤りも訂正する義務を負わず、本情報または製品仕様のアップデートを貴殿または貴社に知らせる義務も負いません。事前の書面による同意のない限り、貴殿または貴社は本情報を再生産、変更、頒布、または公に展示してはなりません。 一定の製品は、ザイリンクスの限定的保証の諸条件に従うこととなるので、http://japan.xilinx.com/legal.htm#tos で見られるザイリンクスの販売条件を参照して下さい。IP コアは、ザイリンクスが貴殿または貴社に付与したライセンスに含まれる保証と補助的条件に従うことになります。 ザイリンクスの製品は、フェイルセーフとして、または、フェイルセーフの動作を要求するアプリケーションに使用するために、設計されたり意図されたりしていません。そのような重大なアプリケーションにザイリンクスの製品を使用する場合のリスクと責任は、貴殿または貴社が単独で負うものです。http://japan.xilinx.com/legal.htm#tos で見られるザイリンクスの販売条件を参照して下さい。

この通知は参照用として、英語版 (XCN15038、バージョン 1.0、2015 年 12 月 21 日リリース) を翻訳したものです。