UltraScale FPGA RSA Authentication and Supporting Configuration Modes

XCN15038 (v1.0) December 21, 2015

Product Change Notice

Overview

The purpose of this notification is to advise customers that the RSA authentication feature for bitstream configuration is limited to selected configuration modes in the Kintex UltraScale and Virtex UltraScale FPGAs.

Description

Loading an RSA authenticated bitstream via an unsupported configuration mode results in an authentication error and the device can lock down or, if enabled, attempt to load a fallback configuration bitstream. Table 1 lists the selected configuration modes that support RSA authentication for configuration bitstreams.

These limitations are present in all Kintex UltraScale and Virtex UltraScale FPGAs but were not previously documented, except for the KU025 device. The UltraScale Architecture Configuration User Guide (UG570), v1.6, has been revised to include the information shown in Table 1.

Table 1: **UltraScale FPGAs and Configuration Modes Supporting RSA Authentication**

Configuration Interface	Data Bus Width	Kintex UltraScale FPGAs				Virtex UltraScale FPGAs		
		KU025(3)	KU035 KU040	KU060 KU085 KU115	KU095	VU080 VU095	VU065 VU125 VU160 VU190	VU440
SelectMAP	32	N/A	Yes(1)	Yes(1)	Yes(1)	Yes(1)	Yes(1)	Yes(1)
	16	N/A	Yes(1)	Yes(1)	Yes(1)	Yes(1)	Yes(1)	Yes(1)
	8	N/A	No	No	Yes(1)	Yes(1)	No	Yes(1)
BPI	16	N/A	Yes	Yes(2)	Yes	Yes	Yes	Yes
	8	N/A	No	No	Yes(2)	Yes(2)	No	Yes
SPI	8	N/A	No	No	Yes	Yes	No	Yes
	4	N/A	No	No	No	No	No	Yes
	2	N/A	No	No	No	No	No	No
	1	N/A	No	No	No	No	No	No
JTAG	1	N/A	No	No	No	No	No	No
Serial	1	N/A	No	No	No	No	No	No

Notes:
1. Not supported if non-continuous SelectMAP data loading is implemented by de-asserting the CSI_B signal.
2. Not supported if asynchronous page read is used.
3. Not applicable to the Kintex UltraScale KU025 FPGA, which has no support for the RSA authentication.

Products Affected

This change affects all speed, package, and temperature variations of the Kintex UltraScale and Virtex UltraScale FPGAs listed in Table 1, and all associated specification control document (SCD) devices.

Traceability

Affected devices are identified by the Kintex UltraScale or Virtex UltraScale family names, or by the corresponding KU or VU device types as highlighted by the blue dashed boxes in Figure 1.

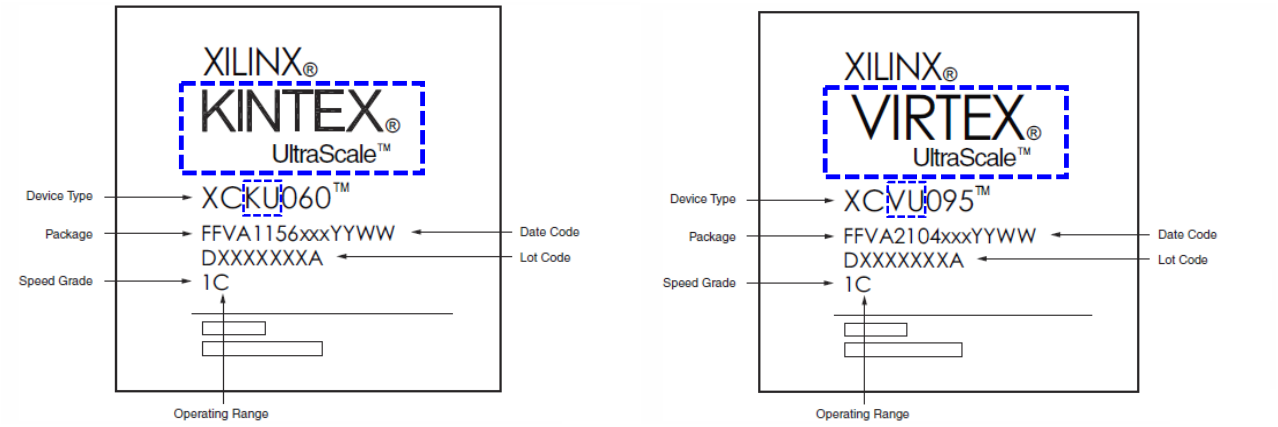

Figure 1: **Example Device Top Marks**

Recommendations

Xilinx recommends customers using RSA authentication review and adjust the FPGA configuration system and board design, as needed, for a supporting configuration mode. See Table 1 in this document or Table 8-1 in UG570 for supported configuration modes and details.

For an alternative configuration bitstream authentication method, the UltraScale FPGAs also support Advanced Encryption Standard (AES) decryption and authentication using the Galois/Counter Mode (GCM) algorithm. The AES-GCM feature is supported in all configuration modes in all Virtex UltraScale and Kintex UltraScale FPGAs including the KU025 FPGA. Based on your security requirements, evaluate if AES-GCM is a suitable alternative. The AES-GCM is a symmetric key encryption algorithm that includes authentication, whereas RSA is an asymmetric authentication algorithm. See UG570 for implications to the FPGA configuration functions when using AES-GCM encryption.

Response

No response is required. For additional information or questions, please contact Xilinx Technical Support.

Important Notice: Xilinx Customer Notifications (XCNs, XDNs, and Quality Alerts) can be delivered via e-mail alerts sent by the Support website (http://www.xilinx.com/support). Register today and personalize your "Documentation and Design Advisory Alerts" area to include Customer Notifications. Xilinx Support provides many benefits, including the ability to receive alerts for new and updated information about specific products, as well as alerts for other publications such as data sheets, errata, application notes, etc. For information on how to sign up, refer to Answer Record 18683: http://www.xilinx.com/support/answers/18683.htm.

Additional Documentation

UltraScale Architecture Configuration User Guide (UG570), v1.6 or later:

http://www.xilinx.com/support/documentation/user_guides/ug570-ultrascale-configuration.pdf

Revision History

The following table shows the revision history for this document:

Date	Version	Description of Revisions
12/21/2015	1.0	Initial release.

Notice of Disclaimer