





Table 2 lists the design requirements for IGLOO2.

**Table 2 • IGLOO2 Design Requirements**

Design Requirements	Description
<b>Hardware Requirements</b>	
IGLOO2 Evaluation Kit (M2GL090S-EVAL-KIT) <ul style="list-style-type: none"> <li>• 12 V adapter (provided along with the kit)</li> <li>• FlashPro4 programmer (provided along with the kit)</li> <li>• M2GL090TS-1FGG484*</li> </ul>	Rev D or later
Host PC or Laptop	Any 64-bit Windows Operating System
<b>Software Requirements</b>	
Liberio SoC	v11.7
<i>Note: * The IGLOO2 design uses the M2GL090TS-1FGG484 device in the IGLOO2 Evaluation Kit. However, the official IGLOO2 Evaluation Kit uses the M2GL010T-1FGG484 device. If you want to run the application note design in the M2GL010T-1FGG484 device, refer to the <b>KB5659</b> for migrating M2GL090TS-1FGG484 to M2GL010T-1FGG484.</i>	

## SmartFusion2 and IGLOO2 NRBG Block Overview

The NRBG block in SmartFusion2 and IGLOO2 has the following two main components:

- A true random entropy source
- A deterministic random bit generator (DRBG), sometimes called a pseudo-random number generator (PRNG)

The entropy source is used to seed DRBG, which can generate many pseudo-random output bits from one seed. The NRBG block in SmartFusion2/IGLOO2 supports all commands defined in NIST SP800-90, such as creating an instantiation, generating random bits, and reseeding. They are supported at a design security strength of 256-bit. Up to 1024 random bits can be returned per call to an instantiation.

The NRBG services are used for design security purposes by the system controller, for example to generate nonces required in the various design security protocols, or to generate ephemeral design-security keys. You can additionally create up to two NRBG instantiations for any purpose, such as for data security applications.

**Note:** Access to the NRBG system services is only available on S version of the devices such as M2S090S and M2GL090TS.

































