INTERPRETATION IC 135-2008-17 OF
ANSI/ASHRAE STANDARD 135-2008 BACnet® -
A Data Communication Protocol for Building
Automation and Control Networks

Approval Date: January 29, 2011

Request from: Dean Matsen (dean.matsen@honeywell.com), Alerton Dealer Business Honeywell Automation & Control Solutions, 6670 185th Ave. NE, Redmond, WA 98052.

Reference: This request for interpretation refers to the requirements presented in Addendum g to ANSI/ASHRAE Standard 135-2008, Clauses 24.15.2.1 (page 45), relating to methods for discovering time.

Background: Clause 24.15.2.1 describes the preferred method of acquiring the time, which involves challenging an unspecified device (presumably any peer device?). This "preferred" procedure is not described in any detail other than to say it involves a challenge.

Clauses 24.15.2.1.1-3 describe three methods in more detail, but these sections are following a clause that implies that cryptographic-quality pseudorandom number generation is required to do any of them (this is the last paragraph of 24.15.2.1, which starts with "other methods for determining time are described below...")

The only attack described in 24.15.2.1 is a replay attack. To avoid a reply in this situation, a device must use a challenge it has never used before. While a crypto-PRNG would do this, it is not the only way to do it. The persistent "next special message ID" scheme described in 24.15.2.1 would work just as well (in fact, maybe BETTER because the PRNG is more likely to suffer from a birthday collision, since the PRNG output gets expressed in the relatively small 32-bit time stamp and/or message ID). In any case, ultimately there is no justification for why the algorithms of 24.15.2.1.1-3 require crypto-PRNG to operate safely.

Based on this, one could argue that any of the mechanisms in Clauses 24.15.2.1.1 through 24.15.2.1.3 can be used safely with either kind of challenge ID/timestamp generator described in 24.15.2.1.

It would be reasonable to guess that an editorial error makes it sound like Clauses 24.15.2.1.1 through 24.15.2.1.3 require the crypto-PRNG described at the end of 24.15.2.1, even though that wasn't intended.

Interpretation No.1: The "preferred" vs. "other" has to do with whether a device is able to store the "next special Message ID" between power cycles. If it can't, then it has to use a crypto-PRNG with entropy, etc... in order to ensure that it doesn't do the same thing on every power up.

Question No.1: Is this interpretation correct?

Answer No.1: Yes.

Interpretation No.2: Clauses 24.15.2.1.1 through 24.15.2.1.3 describe algorithms that can be used with the "preferred" as well as the "other" method of producing unique challenges.

Question No.2: Is this interpretation correct?

Answer No.2: Yes.