INTERPRETATION IC 135-2008-19 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, Clause 24.3.3.3 and Table 24.11 (page 20), relating to What it means for a device to "know a key".

Background: Clause 24.3.3.3 states "The List Of Known Keys is populated with each of the Key Identifiers that the device knows"

This is somewhat vague and very subject to interpretation. There is no given definition of what it means to "know" a key.

It is also not specified whether the Device-Master-Key and/or Distribution-Keys are to be included in the list. Most devices apparently "know" these, but it's useless information to any other device except the key server.

Furthermore, it is not specified whether keys are to be included in the list if they reside in an expired or not-yet-active key set. One could argue that the device apparently "knows" these keys as well, but they are not that useful to the other device at the current time.

There is no indication of what to do if both key sets are simultaneously active. Knowing this is important because it may require the device to compute the union of the key sets.

There is a clause in 24.3.3.3 that states "A device may optionally leave out of the List Of Known Keys any keys that the device knows will not grant sufficient access if the failed action is retried." On the surface, this sounds like optionally leaving weak(er) keys off the list and only including strong(er) keys. However, it could also be possibly interpreted to mean leaving any keys off the list that the other device can't use at all (If the device can't use the key at all, then it won't grant sufficient access).

Given this, it seems that the device "knowing" the key is almost irrelevant. Rather, the list should only include keys the receiver of the error could possibly use, additionally leaving out any known weak(er) keys.

Interpretation: The returned list of "known" keys is to be formulated as follows:

- The Device-Master-Key and Distribution-Key are left off the list

- Only keys from currently active key sets are returned. Keys from expired or not yet active key sets are excluded.

- If both key sets are active, a cheap implementation may just concatenate the two key sets, possibly listing the same key twice. A better implementation may optionally ensure that each key is only listed once.

Question: Is this interpretation correct?

Answer: No.

Comments: The response should only consider keys from the revision used to secure the message. Also the DeviceMaster and Distribution keys should be included due to their use in certain services that can report this error.