INTERPRETATION IC 135-2020-31 OF ANSI/ASHRAE STANDARD 135-2020 BACnet® - A Data Communication Protocol for Building Automation and Control Networks

Approval Date: June 22, 2024

Request from: Stephen Karg, Legrand/BCS, Wattstopper, 739 Jasmine Way, Hoover, AL 35226.

Reference: This request for interpretation refers to ANSI/ASHRAE Standard 135-2020, Clause AB.7.4, relating to Date and Time properties of the Device object.

Background:
ANSI/ASHRAE Standard 135-2020
AB.7.4 Connection Security (excerpt)

The use of secure WebSocket connections as of RFC 6455 and TLS V1.3 as of RFC 8446 for BACnet/SC connections provides for confidentiality, integrity, and authenticity of BVLC messages transmitted across the connection.

The establishment of a secure WebSocket connection shall be performed as defined in RFC 6455. For establishing a secure WebSocket connection, mutual TLS authentication shall be performed. "Mutual authentication" in this context means that both the initiating peer and the accepting peer shall:
…
(b) Validate that the peer's operational certificate is active as of the current date and not expired.
…

RFC 5280 – Internet X.509 Public Key Infrastructure Certificate
and Certificate Revocation List (CRL) Profile (excerpt)
…
4.1.2.5. Validity

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate.
…
In some situations, devices are given certificates for which no good expiration date can be assigned. For example, a device could be issued a certificate that binds its model and serial number to its public key; such a certificate is intended to be used for the entire lifetime of the device.

To indicate that a certificate has no well-defined expiration date, the notAfter SHOULD be assigned the GeneralizedTime value of 99991231235959Z.

BTL-CR-0567_Local_Date-Time Property-SC (excerpt)

The security of BACnet/SC is primarily based on the security of the encryption and signature algorithms of TLS. These do not require a time specification. The time validity restriction of TLS certificates mainly serves the security of the public Internet in order to force providers to maintain their servers and to automatically remove legacy systems with security problems from circulation at some point. However, BACnet/SC networks are not normally part of the public Internet and are inaccessible to third parties without publication of the private keys of the root certificates maintained by the administrator, even without a validity check (security is provided by the signature check against the root certificate). A real-time clock significantly increases the hardware costs (e.g. for battery buffering in the event of a power failure) and the maintenance requirements (configuration) of devices. The administration effort for maintaining the individual real-time clocks in isolated networks without Internet access can be considerable, which further increases the entry hurdle for users in BACnet/SC.

Interpretation: BACnet devices with a BACnet Secure Connect datalink that are designed to only accept certificates for which no good expiration date can be assigned are not required to track time and date, and not required to support Date and Time properties in the Device object.

Question: Is this Interpretation correct?

Answer: No

Comments: A.B.7.4 requires BACnet/SC devices validate that "the peer's operational certificate is active as of the current date and not expired". Clause 12.11 requires that devices capable of tracking time support the Local_Date and Local_Time properties