

Clarification Request

References: ASHRAE 135-2020

Date of BTL-WG Response: May 16, 2024

Background:

Relationship Data-Link-Layer Secure-Connect to 'Local-Date' and 'Local-Time'

135-2020:

...

AB.7.4 Connection Security

...

(b) Validate that the peer's operational certificate is active as of the current date and not expired.

...

Seems to imply, that every BACnet/SC device needs to know current data and time in order to perform that required validation.

135-2020

...

12.11 Device Object Type

...

Footnotes

12 These properties shall be present if the device is capable of tracking date and time.

...

Seem to imply, that the properties local date and local time are required to exist if the device has knowledge about current date and time.

BTL testpackage currently seems to contain no explicit rule for verifying time handling of a device with support for BACnet/SC.

Problem:

The IUT BACnet Rev.18 with Data-Link-Layer Secure-Connect (Hub and Node) without the properties 'Local-Date' and 'Local-Time' (the IUT does not support an internal clock). The manufacturer would like to clarify whether a BTL certificate is possible without these properties.

The manufacturer's arguments:

- 1 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.
- 2 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).

3 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.

4 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.

135.1-2023 - 12.5.2.2.4 - Rejection of Invalid Certificate Incoming Connection Test, the test fails.

Question:

1. Is it possible to certify a BACnet SC device without 'Local-Date' and 'Local-Time' properties?
2. If the answer to question 1 is "yes", may the test 135.1-2023 - 12.5.2.2.4 be skipped?

Response:

1. **No. Clause 12.11 footnote 12 requires local date and time to be present if the device is capable of tracking date and time. This is because BACnet / SC requires the device to validate the current time and date against the operational certificate.**
2. **No. The test cannot be skipped.**