BACnet® TESTING LABORATORIES
ADDENDA

Addendum cd to BTL Test Package 20.0.1

Revision v5
Revised 11/1/2022

Approved by the BTL Working Group on 2022-06-02.
Approved by the BTL Working Group Voting Members on 2022-10-31.
Published on 2022-11-02

[This foreword and the "Overview" on the following pages are not part of this Test Package. They are merely informative and do not contain requirements necessary for conformance to the Test Package.]

FOREWORD

The purpose of this addendum is to present current changes being made to the BTL Test Package. These modifications are the result of change proposals made pursuant to the continuous maintenance procedures and of deliberations within the BTL-WG Committee. The changes are summarized below.

In the following document, language to be added to existing clauses within the BTL Test Package 20.0.1 is indicated through the use of *italics*, while deletions are indicated by ~~strikethrough~~. Where entirely new subclauses are proposed to be added, plain type is used throughout

In contrast, changes to BTL Specified Tests also contain a yellow highlight to indicate the changes made by this addendum. When this addendum is applied, all highlighting will be removed. Change markings on tests will remain to indicate the difference between the new test and an existing 135.1 test. If a test being modified has never existed in 135.1, the applied result should not contain any change markings. When this is the case, square brackets will be used to describe the changes required for this test.

Each addendum can stand independently unless specifically noted via dependency within the addendum. If multiple addenda change the same test or section, each future released addendum that changes the same test or section will note in square brackets whether or not those changes are reflected.

BTL-20.0.1 cd-1: Add Cipher Suite Application Profile Requirements for BACnet/SC [BTLWG-1179]

Overview:

The addendum **135-2020*cd*-1,** TLS V1.3 Cipher Suite Application Profile for BACnet/SC, introduced a required-to-implement TLS V1.3 cipher suite application profile for BACnet/SC. The profile requires support of one TLS cipher suite, one digital signature ECC algorithm, and one elliptic curve for key exchange.

Add into 14.YY, language that states that all of the tests are performed with the TD only supporting the following:

a) TLS cipher suite "TLS_AES_128_GCM_SHA256",
b) digital signature with "ecdsa_secp256r1_sha256", and
c) key exchange with "secp256r1"

unless otherwise directed by the test's Configuration Requirements

Changes:

Checklist Changes

None

Test Plan Changes

None

Specified Test Changes

[Add additional paragraph to section 14.YY]

14.YY Secure Connect Functionality Tests

This clause defines the tests necessary to demonstrate Secure Connect functionality, as defined in Annex YY of the BACnet Standard.

In the diagrams that follow, the following legend applies. Nodes and hub functions are shown within the BACnet device in which they reside by having the circle or rounded square located inside a BACnet device rectangle.

[No changes to the diagram]

Secure Connect differs from other datalinks in that a single network consists of numerous logical connections instead of a shared bus. While the messages do usually exist on a shared ethernet segment, they are described as if each WebSocket is a separate link.

Where it is not clear which WebSocket the messages are expected on, the PORT keyword is used to identify the WebSocket. This construct is mostly used when the IUT has multiple connections such as when it is a hub or participating in direct connections.

Secure Connect implementations in TD shall support TLS version 1.3 only. Unless otherwise directed by the test's Configuration Requirement, the tests shall be executed using the following TLS V1.3 cipher suite application profile. For the definition of the terms in quotes see RFC 8446:

(a) TLS cipher suite "TLS_AES_128_GCM_SHA256",
(b) digital signature with "ecdsa_secp256r1_sha256", and
(c) key exchange with "secp256r1".