BSR/ASHRAE Addendum *cd* to
ANSI/ASHRAE Standard 135-2020

Public Review Draft

Proposed Addendum *cd* to Standard 135-2020, BACnet® - A Data Communication Protocol for Building Automation and Control Networks

First Public Review (??)

This draft has been recommended for public review by the responsible project committee. To submit a comment on this proposed standard, go to the ASHRAE website at www.ashrae.org/standards-research--technology/public-review-drafts and access the online comment database. The draft is subject to modification until it is approved for publication by the Board of Directors and ANSI. Until this time, the current edition of the standard (as modified by any published addenda on the ASHRAE website) remains in effect. The current edition of any standard may be purchased from the ASHRAE Online Store at www.ashrae.org/bookstore or by calling 404-636-8400 or 1-800-727-4723 (for orders in the U.S. or Canada).

This standard is under continuous maintenance. To propose a change to the current standard, use the change submittal form available on the ASHRAE website, www.ashrae.org.

The appearance of any technical data or editorial material in this public review document does not constitute endorsement, warranty, or guaranty by ASHRAE of any product, service, process, procedure, or design, and ASHRAE expressly disclaims such.

© 2020 ASHRAE. This draft is covered under ASHRAE copyright. Permission to reproduce or redistribute all or any part of this document must be obtained from the ASHRAE Manager of Standards, 180 Technology Parkway NW, Peachtree Corners, GA 30092. Phone: 404-636-8400, Ext. 1125. Fax: 404-321-5478. E-mail: standards.section@ashrae.org.

ASHRAE, 1791 Tullie Circle, NE, Atlanta GA 30329-2305

[This foreword, the table of contents, the introduction, and the "rationales" on the following pages are not part of this standard. They are merely informative and do not contain requirements necessary for conformance to the standard.]

FOREWORD

The purpose of this addendum is to present a proposed change for public review. These modifications are the result of change proposals made pursuant to the ASHRAE continuous maintenance procedures and of deliberations within Standing Standard Project Committee 135. The proposed changes are summarized below.

135-2020*cd*-1. TLS V1.3 Cipher Suite Application Profile for BACnet/SC**, p. 3.**

In the following document, language to be added to existing clauses of ANSI/ASHRAE 135-2020 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. Only this new and deleted text is open to comment at this time. All other material in this document is provided for context only and is not open for public review comment except as it relates to the proposed changes.

The use of placeholders like XX, YY, ZZ, X1, X2, NN, x, n, ? etc. should not be interpreted as literal values of the final published version. These placeholders will be assigned actual numbers/letters only after final publication approval of the addendum.

© ASHRAE 2020. All rights reserved.

135-2020*cd*-1. TLS V1.3 Cipher Suite Application Profile for BACnet/SC

Rationale

BACnet/SC (135-2020 Annex AB) mandates TLS v1.3 and leaves it to RFC 8446 to mandate which cipher suites are required to be supported. RFC 8446, in its Clause 9.1, requires support of:

- Cipher Suite TLS_AES_128_GCM_SHA256,
- Digital Signatures with rsa_pkcs1_sha256 (for certificates), rsa_pss_rsae_sha256 (for certificate verify and certificates), and ecdsa_secp256r1_sha256, and
- Key Exchange with secp256r1 (NIST P-256 elliptic curve)

For improved interoperability and less complex implementations, BACnet/SC should define and require a TLS V1.3 cipher suite application profile with reduced requirements than the RFC.

The changes in this section introduce 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. RSA digital signatures are not required in this profile.

[Change **Clause AB.7.4**, p. 1406]

AB.7.4 Connection Security

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:

(a) Validate that the peer's operational certificate is well formed.
(b) Validate that the peer's operational certificate is active as of the current date and not expired.
(c) Validate that the peer's operational certificate is not revoked, if such information is available.
(d) Validate that the peer's operational certificate is directly signed by one of the locally configured CA certificates.

To ensure interoperability, no additional checks beyond the above shall be performed by default, and none are required to be supported. Any additional checks, e.g., Common Name, Distinguished Name, or Subject Alternate Names matches, shall only be performed if specifically enabled, as directed by the installation. The support and update of revocation information is a local matter.

In BACnet/SC, it is assumed that both the initiating and accepting peer of an established WebSocket connection are trusted, including all code they execute. The validation of such code and its origins is outside the scope of this standard.

BACnet/SC implementations shall support TLS version 1.3 as specified in RFC 8446. *BACnet/SC implementations shall support 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".*

Support of other versions of TLS or *other* cipher suites*, digital signatures, or key exchanges* ~~beyond those required by TLS 1.3~~ is a local matter. Additional supported TLS versions*, and additional supported* ~~and~~ cipher suites, *digital signatures, or key exchanges* shall be listed in the PICS. See Annex A.

© ASHRAE 2020. All rights reserved.

[Change **Annex A**, p. 966]

...

☐ Additional cipher suites*, digital signatures, and key exchanges* supported beyond those required for ~~TLS V1.3~~ *the BACnet/SC TLS V1.3 cipher suite application profile defined in Clause AB.7.4*

The additional cipher suites*, digital signatures, or key exchanges* supported using the ~~cipher suite~~ names as of the TLS Cipher Suite Registry at IANA (See RFC 8446):

_____

_____

☐ Additional Transport Layer Security versions other than V1.3 supported

The TLS versions other than V1.3 that are supported, including the supported cipher suites, *digital signatures, and key exchanges* for the version ~~beyond those required~~, using the ~~cipher suite~~ names as defined by the TLS version supported:

_____

_____

☐ Generates private keys internally, and provides matching certificate signing requests.

...

© ASHRAE 2020. All rights reserved.

[Add a new entry to **History of Revisions**, p. 1429]

(This History of Revisions is not part of this standard. It is merely informative and does not contain requirements necessary for conformance to the standard.)

HISTORY OF REVISIONS

…	…	**…**
1	X	**Addendum *cd* to ANSI/ASHRAE 135-2020** Approved by the ASHRAE Standards Committee MONTH X, 20XX; by the ASHRAE Board of Directors MONTH X, 20XX; and by the American National Standards Institute MONTH X, 20XX. 1. TLS V1.3 Cipher Suite Application Profile for BACnet/SC

© ASHRAE 2020. All rights reserved.