ADDENDA

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

BACnet™

A Data Communication Protocol for Building Automation and Control Networks

Approved by ASHRAE and the American National Standards Institute on August 31, 2021.

This addendum was approved by a Standing Standard Project Committee (SSPC) for which the Standards Committee has established a documented program for regular publication of addenda or revisions, including procedures for timely, documented, consensus action on requests for change to any part of the standard. Instructions for how to submit a change can be found on the ASHRAE® website (https://www.ashrae.org/continuous-maintenance).

The latest edition of an ASHRAE Standard may be purchased on the ASHRAE website (www.ashrae.org) or from ASHRAE Customer Service, 180 Technology Parkway NW, Peachtree Corners, GA 30092. E-mail: orders@ashrae.org. Fax: 678-539-2129. Telephone: 404-636-8400 (worldwide), or toll free 1-800-527-4723 (for orders in US and Canada). For reprint permission, go to www.ashrae.org/permissions.

 ISSN 1041-2336

Approved American National Standard
ANSI
www.ansi.org

SPECIAL NOTE

This American National Standard (ANS) is a national voluntary consensus Standard developed under the auspices of ASHRAE. *Consensus* is defined by the American National Standards Institute (ANSI), of which ASHRAE is a member and which has approved this Standard as an ANS, as "substantial agreement reached by directly and materially affected interest categories. This signifies the concurrence of more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that an effort be made toward their resolution." Compliance with this Standard is voluntary until and unless a legal jurisdiction makes compliance mandatory through legislation.

ASHRAE obtains consensus through participation of its national and international members, associated societies, and public review.

ASHRAE Standards are prepared by a Project Committee appointed specifically for the purpose of writing the Standard. The Project Committee Chair and Vice-Chair must be members of ASHRAE; while other committee members may or may not be ASHRAE members, all must be technically qualified in the subject area of the Standard. Every effort is made to balance the concerned interests on all Project Committees.

The Senior Manager of Standards of ASHRAE should be contacted for

a. interpretation of the contents of this Standard,
b. participation in the next review of the Standard,
c. offering constructive criticism for improving the Standard, or
d. permission to reprint portions of the Standard.

[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.

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.

[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.

...

[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	23	**Addendum *cd* to ANSI/ASHRAE 135-2020** Approved by ASHRAE and the American National Standards Institute on August 31, 2021. 1. TLS V1.3 Cipher Suite Application Profile for BACnet/SC

POLICY STATEMENT DEFINING ASHRAE'S CONCERN FOR THE ENVIRONMENTAL IMPACT OF ITS ACTIVITIES

ASHRAE is concerned with the impact of its members' activities on both the indoor and outdoor environment. ASHRAE's members will strive to minimize any possible deleterious effect on the indoor and outdoor environment of the systems and components in their responsibility while maximizing the beneficial effects these systems provide, consistent with accepted Standards and the practical state of the art.

ASHRAE's short-range goal is to ensure that the systems and components within its scope do not impact the indoor and outdoor environment to a greater extent than specified by the Standards and Guidelines as established by itself and other responsible bodies.

As an ongoing goal, ASHRAE will, through its Standards Committee and extensive Technical Committee structure, continue to generate up-to-date Standards and Guidelines where appropriate and adopt, recommend, and promote those new and revised Standards developed by other responsible organizations.

Through its *Handbook*, appropriate chapters will contain up-to-date Standards and design considerations as the material is systematically revised.

ASHRAE will take the lead with respect to dissemination of environmental information of its primary interest and will seek out and disseminate information from other responsible organizations that is pertinent, as guides to updating Standards and Guidelines.

The effects of the design and selection of equipment and systems will be considered within the scope of the system's intended use and expected misuse. The disposal of hazardous materials, if any, will also be considered.

ASHRAE's primary concern for environmental impact will be at the site where equipment within ASHRAE's scope operates. However, energy source selection and the possible environmental impact due to the energy source and energy transportation will be considered where possible. Recommendations concerning energy source selection should be made by its members.

ASHRAE · 180 Technology Parkway NW · Peachtree Corners, GA 30092 · www.ashrae.org

About ASHRAE

Founded in 1894, ASHRAE is a global professional society committed to serve humanity by advancing the arts and sciences of heating, ventilation, air conditioning, refrigeration, and their allied fields.

As an industry leader in research, standards writing, publishing, certification, and continuing education, ASHRAE and its members are dedicated to promoting a healthy and sustainable built environment for all, through strategic partnerships with organizations in the HVAC&R community and across related industries.

To stay current with this and other ASHRAE Standards and Guidelines, visit www.ashrae.org/standards, and connect on LinkedIn, Facebook, Twitter, and YouTube.

Visit the ASHRAE Bookstore

ASHRAE offers its Standards and Guidelines in print, as immediately downloadable PDFs, and via ASHRAE Digital Collections, which provides online access with automatic updates as well as historical versions of publications. Selected Standards and Guidelines are also offered in redline versions that indicate the changes made between the active Standard or Guideline and its previous version. For more information, visit the Standards and Guidelines section of the ASHRAE Bookstore at www.ashrae.org/bookstore.

IMPORTANT NOTICES ABOUT THIS STANDARD

To ensure that you have all of the approved addenda, errata, and interpretations for this Standard, visit www.ashrae.org/standards to download them free of charge.

Addenda, errata, and interpretations for ASHRAE Standards and Guidelines are no longer distributed with copies of the Standards and Guidelines. ASHRAE provides these addenda, errata, and interpretations only in electronic form to promote more sustainable use of resources.

8/21