IEEE P802.1AEa/D0.1

Draft Standard for Local and Metropolitan Area Networks—

Media Access Control (MAC) Security — Amendment 1: GCM-AES-256 Cipher Suite

Sponsor
LAN/MAN Standards Committee of the IEEE Computer Society

Prepared by the Security Task Group of IEEE 802.1
This initial draft has been prepared by the Task Group Chair to facilitate discussion of a possible PAR and has no official standing whatsoever.

Abstract: This amendment specifies the GCM-AES-256 Cipher Suite as an option in addition to the existing mandatory to implement Default Cipher Suite, GCM-AES-128.
Keywords: authorized port, confidentiality, data origin authenticity, integrity, LANs, local area networks, MAC Bridges, MAC security, MAC Service, MANs, metropolitan area networks, port based network access control, secure association, security, transparent bridging.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 13 31
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Editors' Foreword

<<Notes>>

<<Throughout this document, all notes such as this one, presented between angle braces, are temporary notes inserted by the Editors for a variety of purposes; these notes and the Editors' Foreword will all be removed prior to publication and are not part of the normative text.>>

<<Comments and participation in 802.1 standards development

Comments on this draft are encouraged. **PLEASE NOTE: All issues related to IEEE standards presentation style, formatting, spelling, etc. are routinely handled between the 802.1 Editor and the IEEE Staff Editors prior to publication, after balloting and the process of achieving agreement on the technical content of the standard is complete.** Readers are urged to devote their valuable time and energy only to comments that materially affect either the technical content of the document or the clarity of that technical content. Comments should not simply state what is wrong, but also what might be done to fix the problem.>>

Full participation in the development of this draft requires individual attendance at IEEE 802 meetings. Information on 802.1 activities, working papers, and email distribution lists etc. can be found on the 802.1 Website:

http://ieee802.org/1/

Use of the email distribution list is not presently restricted to 802.1 members, and the working group has had a policy of considering ballot comments from all who are interested and willing to contribute to the development of the draft. Individuals not attending meetings have helped to identify sources of misunderstanding and ambiguity in past projects. Non-members are advised that the email lists exist primarily to allow the members of the working group to develop standards, and are not a general forum. All contributors to the work of 802.1 should familiarize themselves with the IEEE patent policy and anyone using the mail distribution will be assumed to have done so. Information can be found at http://standards.ieee.org/db/patents/

Comments on this document may be sent to the 802.1 email exploder, to the Editor, or to the Chairs of the 802.1 Working Group and Interworking Task Group.

t.b.d
Editor, P802.1AEa
Email:

Mick Seaman
Chair, 802.1 SecurityTask Group
Email:mick_seaman@sbcglobal.net

Co-Editor P802.1aq

Tony Jeffree
Chair, 802.1 Working Group
11A Poplar Grove
Sale, Cheshire, M33 3AX, UK
+44 161 973 4278 (Tel)
+44 161 973 6534 (Fax)
Email: tony@jeffree.co.uk

PLEASE NOTE: Comments whose distribution is restricted in any way cannot be considered, and may not be acknowledged.>>

<<Overview: Draft text and accompanying information

This document currently comprises:

A cover page, identical to the title page.
The editors' introductory notes to each draft, briefly summarizing the progress and focus of each successive draft.
The title page for this amendment including an Abstract and Keywords. This title page will be retained for the period that the amendment is published as a separate document.
The amendment proper, documented in the usual form for amendments to 802 standards; i.e., as an explicit set of editing instructions that, if correctly applied to the text of 802.1Q, will create a corrected document.
An Annex Z comprising the editors' discussion of issues. This annex will be deleted from the document prior to sponsor ballot.
Editors' notes throughout the document, including requests for comment on specific issues and pointing deficiencies in the current draft.
IEEE boilerplate text.

The records of participants in the development of the standard, the introduction to 802 standards, and the introduction to this revision of the standard are not included, and will be added at an appropriate time.

During the early stages of draft development, 802.1 editors have a responsibility to attempt to craft technically coherent drafts from the resolutions of ballot comments and the other discussions that take place in the working group meetings. Preparation of drafts often exposes inconsistencies in editor's instructions or exposes the need to make choices between approaches that were not fully apparent in the meeting. Choices and requests by the editors' for contributions on specific issues will be found in the editors' introductory notes to the current draft, at appropriate points in the draft, and in Annex Z. Significant discussion of more difficult topics will be found in the last of these.

The ballot comments received on each draft, and the editors' proposed and final disposition of comments on working group drafts, are part of the audit trail of the development of the standard and are available, along with all the revisions of the draft on the 802.1 website (for address see above).

During the early stages of draft development the proposed text can be moved around a great deal, and even minor rearrangement can lead to a lot of 'change', not all of which is noteworthy from the point of the reviewer, so the use of automatic change bars is not very effective. In this draft change bars have been manually applied, with a view to drawing the readers attention to the most significant areas of change. Readers interested in viewing every change are encouraged to used Adobe Acrobat to compare the document with their selected prior draft.
>>

<<Editor's Introduction to the current draft.

P802.1AEa/D0.1 has been prepared by the Task Group Chair purely to facilitate discussion of a proposed project.

>>

<<Editor's Introduction to prior drafts (excerpts of continuing relevance).

The current draft is the first.

>>

<<Project Authorization Request, Scope, Purpose, and Five Criteria

A PAR (Project Authorization Request) for this project is under discussion.

Scope of Proposed Project:

<>.

Purpose of Proposed Project:

<>.

Reason:

<>.

1. Broad Market Potential

A standards project authorized by IEEE 802 shall have a broad market potential. Specifically, it shall have the potential for:

a) Broad sets of applicability.
b) Multiple vendors and numerous users
c) Balanced costs (LAN versus attached stations)
<>

2. Compatibility

IEEE 802 defines a family of standards. All standards shall be in conformance with the IEEE 802.1 Architecture, Management and Interworking documents as follows: 802 Overview and Architecture, 802.1D, 802.1Q and parts of 802.1f. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with 802.

Each standard in the IEEE 802 family of standards shall include a definition of managed objects which are compatible with systems management standards.

<>.
Equipment conforming to the proposed amendment to IEEE Std 802.1Q will be compatible and interoperable with bridge implementations that conform to IEEE Std 802.1D and prior revisions of IEEE Std 802.1Q, and support of existing network configurations will be retained in parallel with use of the additional capabilities provided by this amendment. No change to end stations will be required to take advantage of these capabilities.
<>.

3. Distinct Identity

Each IEEE 802 standard shall have a distinct identity. To achieve this, each authorized project shall be:

a) Substantially different from other IEEE 802 standards.
<>
b) One unique solution per problem (not two solutions to a problem).
<>.
c) Easy for the document reader to select the relevant specification.
<>

For a project to be authorized, it shall be able to show its technical feasibility. At a minimum, the proposed project shall show:

a) Demonstrated system feasibility.
<>.
b) Proven technology, reasonable testing.
<>.
c) Confidence in reliability.
<>.

5. Economic Feasibility

For a project to be authorized, it shall be able to show economic feasibility (so far as can reasonably be estimated), for its intended applications. At a minimum, the proposed project shall show:

a) Known cost factors, reliable data.
<>.
b) Reasonable cost for performance.
<>.
c) Consideration of installation costs.
<>.

>>

<<Editors' final checklist (items noted in development, to be applied to final text.

The published standards are inconsistent and a bit of a mess when it comes to PDF bookmarks, this makes using them rather than final working group text difficult. P802.1p/D9 was very good. In particular it provides bookmarks for all figures at the end of a clause (see clause 7 for an example), need to copy that example.
>>

IEEE P802.1AEa/D0.1

Draft Standard for Local and Metropolitan Area Networks—

Media Access Control (MAC) Security — Amendment 1: GCM-AES-256 Cipher Suite

Sponsor
LAN/MAN Standards Committee of the IEEE Computer Society

Prepared by the Security Task Group of IEEE 802.1

Abstract: This amendment specifies the GCM-AES-256 Cipher Suite as an option in addition to the existing mandatory to implement Default Cipher Suite, GCM-AES-128.
Keywords: authorized port, confidentiality, data origin authenticity, integrity, LANs, local area networks, MAC Bridges, MAC security, MAC Service, MANs, metropolitan area networks, port based network access control, secure association, security, transparent bridging.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Introduction

This introduction is not part of IEEE Std 802.1AE, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.

The first edition of IEEE Std 802.1AE was published in 2006. This first amendment to that standard adds the option of using the GCM-AES-256 Cipher Suite.

Relationship between IEEE Std 802.1AE and other IEEE Std 802 standards

IEEE Std 802.1X-2010 specifies Port-based Network Access Control, and provides a means of authenticating and authorizing devices attached to a LAN, and includes the MACsec Key Agreement protocol (MKA) necessary to make use of IEEE 802.1AE.

This standard is not intended for use with IEEE Std 802.11 Wireless LAN Medium Access Control. An amendment to that standard, IEEE Std 802.11i-2004, also makes use of IEEE Std 802.1X, thus facilitating the use of a common authentication and authorization framework for LAN media to which this standard applies and for Wireless LANs.

Notice to users

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Contents

Figures

Tables

IEEE P802.1AEa/D0.1

Draft Standard for Local and Metropolitan Area Networks—

Media Access Control (MAC) Security —Amendment 1: GCM-AES-256 Cipher Suite

Editorial Note

This amendment specifies changes to IEEE Std 802.1Q that allow bridged frames to travel on the shortest path between their source and destination(s). Changes are applied to the base text of IEEE Std 802.1Q-2005 as amended by IEEE Std 802.1ad-2005, IEEE Std 802.1ag-2007, IEEE Std802.1ak-2007, P802.1ah, and P802.1aj. Text shown in bold italics in this amendment defines the editing instructions necessary to changes to this base text. Three editing instructions are used: ***change***, ***delete***, and ***insert***. ***Change*** is used to make a change to existing material. The editing instruction specifies the location of the change and describes what is being changed. Changes to existing text may be clarified using ~~strikeout~~ markings to indicate removal of old material, and underscore markings to indicate addition of new material). ***Delete*** removes existing material. ***Insert*** adds new material without changing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. Editorial notes will not be carried over into future editions of IEEE Std. 802.1Q.

<<The current draft makes no reference to the following clauses which are believed to be unaffected by this amendment:

4. Abbreviations and acronyms
5. Conformance
8. MAC Security Protocol (MACsec)
9. Encoding of MACsec protocol data units
10. Principles of MAC Security Entity (SecY) operation
11. MAC Security in Systems
12. MACsec and EPON
13. Management protocol

Annex A (normative) PICS Proforma
Annex B (informative) Bibliography

>>

1. Overview

This amendment makes no changes to the initial text of Clause 1 Overview.

1.1 Introduction

<Change reference to P802.1af>:

1.2 Scope

<Change reference to P802.1af in two places>:

2. Normative references

Insert the following references at the appropriate point:

IEEE Std 802.1X-2010, IEEE Standards for Local and Metropolitan Area Networks: Port-based Network Access Control.

IEEE Std 802.1Q-201?, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.

Delete the following references:

IEEE Std 802.1Q-2005, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.

IEEE Std 802.1ad-2005, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges.

IEEE Std 802.1X-2004, IEEE Standards for Local and Metropolitan Area Networks: Port Based Network Access Control.

6. Secure provision of the MAC Service

6.7 MACsec connectivity

In the first paragraph replace:

"IEEE P802.1af"

with:

"IEEE Std 802.1X"

7. Principles of secure network operation

In bullet (d) replace:

"IEEE P802.1af"

with:

"IEEE Std 802.1X"

14. Cipher Suites

This amendment currently contains not only the proposed new clause 14.6, but also the full text of clause 14.5 (GCM-AES-128) on which the new clause is based. The latter, though not formally necessary for the purpose of amending IEEE Std 802.1AE was included in the process of preparing this amendment to facilitate techanical and textual alignment of the two clauses and has been retained so that points of similarity and difference are readily apparent to the reader of this amendment.

Modify Table 14-1 as follows:

Table 14-1—MACsec Cipher Suites

Cipher Suite #	Cipher Suite Name	Services provided		Mandatory/Optional	Defining Clause
		Integrity without confidentiality	Integrity and confidentiality		
00-80-02-00-01-00-00-01	GCM–AES–128	Yes	Yes	Mandatory	14.5
00-80-02-00-01-00-00-02	GCM-AES-256	Yes	Yes	Optional	14.6

Delete the NOTE "Currently, ... does not include any optional Cipher suites" following Table 14-1.

Change the introductory paragraph of clause 14.5 as follows:

14.5 Default Cipher Suite (GCM–AES–128)

The Default Cipher Suite uses the Galois/Counter Mode of Operation with the AES-128 symmetric block cipher, as specified in this clause by reference to the terms *K, IV, A, P, C, T* used ~~in section 2.1 of the GCM specification (GCM) as submitted to NIST~~ <updated reference>.

K is the 128 bit SAK. The 64 most significant bits of the 96-bit *IV* are the octets of the SCI, encoded as a binary number (9.1). The 32 least significant bits of the 96--bit *IV* are the octets of the PN, encoded as a binary number (9.1). *T* is the ICV, and is 128 bits long. When the bit-strings *A*, *P*, and *C* are specified in terms of octet strings, earlier octets compose earlier bits, and more significant bits in each octet are earlier.

NOTE—The bit strings obtained by transforming MAC Address and data octets using these rules do not correspond to 802.3 'wire order' for frame transmission.

When the Default Cipher Suite is used for Integrity Protection

- *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and User Data concatenated in that order.
- *P* is null.
- The Secure Data is the octets of the User Data, without modification.

When the Default Cipher Suite is used for Confidentiality Protection without a confidentiality offset

- *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG concatenated in that order.
- *P* is the octets of the User Data.
- The Secure Data is *C*.

When the Default Cipher Suite is used for Confidentiality Protection with a confidentiality offset

- *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and the first confidentialityOffset (10.7.24) octets of the User Data concatenated in that order.
- *P* is the remaining octets of the User Data.
- The Secure Data is the first confidentialityOffset octets of the User Data concatenated with *C,* in that order.

Add clause 14.6 as follows (note that this is not quite right yet- Mick):

14.6 Default Cipher Suite (GCM–AES–256)

GCM-AES-256 uses the Galois/Counter Mode of Operation with the AES-256 symmetric block cipher, as specified in this clause by reference to the terms *K, IV, A, P, C, T* used ~~in section 2.1 of the GCM specification (GCM) as submitted to NIST~~ <updated reference>.

K is the 256 bit SAK. The 64 most significant bits of the 96-bit *IV* are the octets of the SCI, encoded as a binary number (9.1). The 32 least significant bits of the 96--bit *IV* are the octets of the PN, encoded as a binary number (9.1). *T* is the ICV, and is 128 bits long. When the bit-strings *A*, *P*, and *C* are specified in terms of octet strings, earlier octets compose earlier bits, and more significant bits in each octet are earlier.

NOTE—The bit strings obtained by transforming MAC Address and data octets using these rules do not correspond to 802.3 'wire order' for frame transmission.

When the Default Cipher Suite is used for Integrity Protection

- *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and User Data concatenated in that order.
- *P* is null.
- The Secure Data is the octets of the User Data, without modification.

When the Default Cipher Suite is used for Confidentiality Protection without a confidentiality offset

- *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG concatenated in that order.
- *P* is the octets of the User Data.
- The Secure Data is *C*.

When the Default Cipher Suite is used for Confidentiality Protection with a confidentiality offset

- *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and the first confidentialityOffset (10.7.24) octets of the User Data concatenated in that order.

— *P* is the remaining octets of the User Data.
— The Secure Data is the first confidentialityOffset octets of the User Data concatenated with *C,* in that order.

Annex Z

(informative) Temporary, not for publication

Commentary

This is a temporary Annex, a place to record outstanding or recent technical issues and their disposition. It will be removed prior to Sponsor Ballot. Because this is not a part of the proposed standard the editor will not accept comments on the text of this Annex itself, only on the issues raised. Discussion and resolution of the issues will result in modification of the contents.

The order of discussion of issues is intended to help the reader understand first what is the draft, secondly what may be added, and thirdly what has been considered but will not be included. In pursuit of this goal, issues where the proposed disposition is "no change" will be moved to the end. The description of issues is updated to reflect our current understanding[1] of the problem and its solution: where it has been considered useful to retain an original comment, in whole or part, either to ensure that its author does not feel that it has not been sufficiently argued or the editor suspects there may be further aspects to the issue, that has been done as a footnote.

Z.1 Deficiencies in 802.1AE-2006

The following deficiency was noticed during the development of IEEE Std 802.1X-2010. It would directly affect use of this amendment, as well as existing uses of 802.1AE. Corrective text has not yet been added to this amendment.

1AE 10.5.2 correctly states that the value of nextPN for a transmitSA is set, via the LMI, prior to the use of that SA and 10.7.21 provides this capability. Unfortunately the capability to read the nextPN value, which is required for the intended use, is missing from 10.7.22 although it appears as a readable parameter in Figure 10-6. The value is in the MIB. We need to correct 10.7.22.

[1]This annex is not intended therefore to be a complete historical record of the development of the draft. The formal record comprises the retained drafts and dispositions of comments.