Messaging Layer Security
Internet-Draft
Intended status: Standards Track
Expires: 8 November 2026

F. Kiefer
K. Bhargavan
Cryspen
R. L. Barnes
Cisco
J. Alwen
M. Mularczyk
AWS Wickr

7 May 2026

Partial MLS
draft-ietf-mls-partial-02

Abstract

The Messaging Layer Security (MLS) protocol provides efficient asynchronous group key establishment for large groups with up to thousands of clients. In MLS, any member can commit a change to the group, and consequently, all members must download, validate, and maintain the full group state, which can incur a significant communication and computational costs, especially when joining a group. This document defines an MLS extension to support "partial MLS clients" that don’t undertake these costs. A partial client cannot commit changes to the group, and only has partial authentication information for the other members of the group, but is otherwise able to participate in the group. In exchange for these limitations, a partial MLS client can participate in an MLS group with significantly lower requirements in terms of download, memory, and processing.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-mls-partial/.

Discussion of this document takes place on the Messaging Layer Security Working Group mailing list (mailto:mls@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/mls/. Subscribe at https://www.ietf.org/mailman/listinfo/mls/.

Source for this draft and an issue tracker can be found at https://github.com/mlswg/mls-partial.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Messaging Layer Security protocol [RFC9420] enables continuous group authenticated key exchange among a group of clients. The design of MLS requires all members to download, validate, and maintain the full MLS tree, including validating the credentials and signatures of all members. The size of the MLS tree is linear in the size of the group. Consequently, the MLS design results in a performance bottleneck for new members seeking to join a large group, and significant storage and memory requirements once the member has joined.

This document defines an extension to MLS to allow for "partial clients" -- clients that do not download, validate, or maintain the entire ratchet tree for the group. On the one hand, this property allows a partial client to participate in the group with much significantly lower communication and computation complexity. On the other hand, without the full ratchet tree, the partial client cannot create Commit messages to put changes to the group into effect. Partial clients also only have authentication information for the parts of the tree they download, not the whole group.

This document does not change the core logic of MLS, including: The structure of the ratchet tree and its associated algorithms, the key schedule, the secret tree, and application message protection. The messages sent and received by normal clients in the course of an MLS session are likewise unchanged. With proper modifications to the MLS Delivery Service, standard MLS clients can participate in a group with partial clients without any modification.

The only modifications this document makes are to the local state stored at partial clients, namely the component of MLS that manages, synchronizes, and authenticates the public group state. We also defines some "annotations" that need to be appended to group messages so that they can be processed by partial clients. Partial clients effectively run normal MLS algorithms, but with just-in-time delivery of exactly the subset of the public group state needed by a given algorithm. We achieve this property due to the fact that aside from initial tree validation and sending commits, a client only needs log-scale information.

In summary, Partial MLS allows partial clients to obtain greater efficiency, at the cost of lowering the authentication guarantees they receive and losing the ability to make Commits. We discuss a few scenarios that motivate this trade-off in Section 3. The difference in authentication properties, in particular, is discussed in detail in Section 13.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Tree slice: A tree slice is the direct path from a leaf node to the root, together with the tree hashes on the co-path.

Membership proof: A tree slice that proves that a given leaf node is part of a ratchet tree with a given tree hash.

Partial client: An MLS client that does not download, validate, and maintain a copy of the group’s ratchet tree. A partial client does not store any public data about the group’s ratchet tree, only the HPKE decryption keys associated to nodes on the client’s direct path.

Full client: A normal MLS client, in possession of the full MLS ratchet tree for the group.

Sender-authenticated message: A signed MLS message such as Welcome or PublicMessage, together with a membership proof that proves the sender’s membership in the group.

Annotated Welcome: A Welcome message together with information that a partial client needs to process it.

Annotated Commit: A Commit message (as a PublicMessage or PrivateMessage) together with information that a partial client needs to process it.

As in MLS, message structures are defined using the TLS presentation syntax [RFC8446]. Unlike most MLS messages, however, these structures are not encapsulated in a signed or MAC'ed structure. So it may be more convenient for applications to encode these structures in application-specific encodings.

3. Use Cases

Partial MLS is intended to support use cases where MLS groups are very large, from thousands to millions of participants. Application-level constraints arising from these use cases align well with the trade-offs introduced by Partial MLS. It is usually acceptable (even desirable) that only certain members are able to send Commit messages. And in such large groups, clients often do not care about authenticating all members of the group.

The following subsections outline two concrete use cases.

3.1. Large Meetings / Webinars

MLS can be used to establish end-to-end encryption keys in real-time conferencing scenarios. In such scenarios, a client joins the MLS group when they are admitted to a meeting. With normal MLS, the client is required to download and validate the entire ratchet tree before being able to derive media encryption keys. In meetings with a thousand or more participants, this process can take enough time that it introduces a noticeable delay in joining the meeting. If a client joins as a partial client, then they can download a log-sized AnnotatedWelcome message and immediately obtain the media encryption keys.

Such a client will not have authenticated the group when they join the meeting. However, applications often do not display identity information in such setting anyway. In "webinar" settings, it is common for attendee identities to be visible only to panelists and administrators, not to other attendees. Partial MLS allows MLS to align with this privacy property. If attendees join as partial clients, they can be provided with membership proofs for attendees whom they are authorized to see, and not for others. Even in settings where attendees can all see each others' identities, user interface constraints usually cause only a small fraction of the attendee list to be visible at one time, so it is natural to load the tree dynamically as the client needs access to the authenticated identities of specific other clients.

The constraint on clients sending Commits is also natural here. In such large gatherings, there are usually administrators who are authorized to see the identities of all participants and control who is in the group, and conversely, there are certain actions that are not available to non-admin participants. So it makes sense for the administrators to use full clients that are able to make Commits to implement the actions they are authorized to take, and for more limited clients to be unable to make commits.

3.2. Broadcast sessions

Internet streaming platforms frequently host broadcasts with large numbers of viewers, but the entities providing these broadcasts might like to ensure that the streaming platform cannot see the streamed content. For example, the Media over QUIC Transport protocol, designed to support streaming use cases, states as a goal ensuring that "the media content itself remains opaque and private" from the relays involved in its distribution [I-D.ietf-moq-transport].

In such settings, the partial client / full client roles align with the viewer / owner roles, respectively. Viewers do not care about the identities of other viewers (at most, they care that the stream comes from an authentic source) and they aren’t authorized to do anything in MLS besides join the group. Viewers are also typically in more constrained situations than the source of a stream. So the reduced resource requirements are well worth the loss of full-group authentication and the ability to Commit.

4. Protocol Overview

A partial client does not receive or validate a full copy of the ratchet tree for a group, but still possesses the group’s secrets, including receiving updated secrets as the group evolves. When MLS messages are sent to a partial client, they need to be accompanied by annotations that provide the partial client with just enough of information about the ratchet tree to process the message. These annotations can be computed by any party with knowledge of the group’s ratchet tree, including the committer and sometimes the DS.

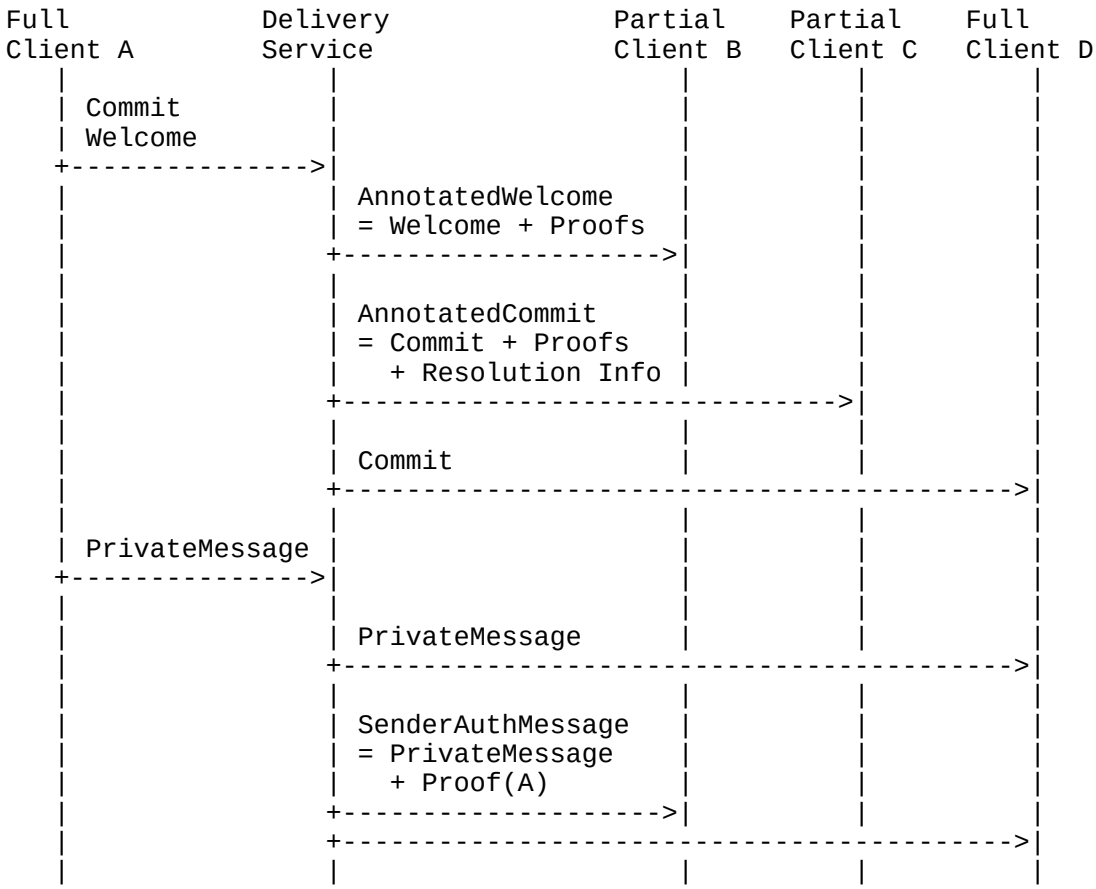

Figure 1: Overview of Partial MLS

Figure 1 illustrates the main changes introduced by Partial MLS:

1. When a partial client is added to the group, they are provided an AnnotatedWelcome message, which comprises a normal Welcome message plus membership proofs for the sender and joiner.

2. From each Commit that is generated in the group, an individual AnnotatedCommit is generated for each partial client. An AnnotatedCommit comprises a normal MLS Commit message, together with membership proofs and the information that the partial client needs in order to process the update path in the Commit.

3. When messages are sent in the group, e.g., carrying application data, they are extended with a membership proofs so that partial clients can authenticate the sender’s membership in the group.

In this example, we have shown the required annotations being added by the DS. This allows full clients to behave as they would in normal MLS, but requires that the DS maintain a copy of the group's ratchet tree. It is also possible for committers to generate the required annotated messages. This document does not define who generates annotated messages from the base MLS messages, or how this entity learns which clients are partial or full clients.

Partial clients still need to be provided with access to any proposals sent in a group outside of Commits. Partial clients cannot process proposals that modify the structure of the tree, in particular Add, Update, or Remove proposals. They can, however, verify that these proposals were included in a given Commit. And they need to see proposals such as PreSharedKey or GroupContextExtensions so that they can update their state appropriately.

Depending on how Partial MLS is deployed, a client might need to inform the DS or other members of its status (partial or full), so that the proper annotations can be generated when it is partial. It is harmless for a full client to receive an AnnotatedCommit; the annotations can simply be ignored.

5. Upgrading and Downgrading

A partial client can upgrade to being a full client at any time by downloading the full ratchet tree; a full client can downgrade by deleting its local copy of the ratchet tree. Before a partial client uses a copy of the ratchet tree to upgrade to being a full client, it MUST verify the integrity of the ratchet tree in the same way it would when joining as a full client, following the steps in Section 12.4.3.1 of [RFC9420].

6. Membership Proofs and Partial Trees

Although partial clients do not have a copy of the group's ratchet tree, they still agree on the root tree hash of the ratchet tree, via the MLS key schedule as usual. This fact, together with the Merkle-tree-like structure of the MLS tree hash, allows a partial client to verify the legitimacy of partial information about the ratchet tree. In particular, for any leaf in the tree, anyone in possession of the public data of the ratchet tree can construct a "membership proof" that proves that a leaf node with specific contents is located at a specific leaf index in the tree.

A membership proof for a leaf node comprises:

* The number of leaves in the tree.

* The leaf index of the member’s leaf.

* The values of the nodes from the leaf node to the root of the tree, including both the leaf node and the root.

* The tree hash values for the nodes on the copath of the leaf node.

```
struct {
    opaque hash_value<V>;
} CopathHash;

struct {
  uint32 leaf_index;
  uint32 n_leaves;
  optional<Node> direct_path_nodes<V>;
  CopathHash copath_hashes<V>;
} MembershipProof;
```

From these values, the root tree hash of the ratchet tree can be recomputed, following the same recursive algorithm specified in Section 7.8 of [RFC9420]. The selection of nodes and subtree hashes provides the precise collection of inputs required by the algorithm.

A membership proof is said to be valid relative to a given tree hash if the tree hash recomputed in this way is equal to the given tree hash.

Two membership proofs are said to reference the same tree if their n_leaves fields are equal, and they produce identical root tree hashes.

7. Sender-Authenticated Messages

For several types of message, MLS authenticates that a message was created by the member at a specific leaf node of the group’s ratchet tree by signing the message with the private key corresponding to the signature_key in the leaf node. Full clients verify these messages by looking up the required signature verification key in their local copy of the ratchet tree.

Since partial clients do not store the group’s ratchet tree, they cannot perform this lookup. A SenderAuthenticatedMessage presents a message along with a membership proof for the sender of a message, which provides the required leaf node and a proof of its inclusion in the tree.

```
struct {
    T message;
    MembershipProof sender_membership_proof;
} SenderAuthenticatedMessage<T>;
```

Before using the sender_membership_proof to verify the included message, a client processing a SenderAuthenticatedMessage MUST verify that the proof is valid relative to the group's tree hash for the epoch in which the message was sent. For a PublicMessage or PrivateMessage, this is the tree hash for the epoch indicated in the FramedContent. For a GroupInfo or Welcome, it is the tree hash in the object itself.

8. Joining via Annotated Welcome

An AnnotatedWelcome message provides a client joining a group with membership proofs for the sender and the joiner (i.e., the recipient of the message).

```
struct {
    SenderAuthenticatedMessage<Welcome> welcome;
    MembershipProof joiner_membership_proof;
} AnnotatedWelcome;
```

The fields in the AnnotatedWelcome have the following semantics:

welcome: A Welcome message, together with a membership proof for the sender relative to the ratchet tree specified in the Welcome.

joiner_membership_proof: A proof of the receipient's membership in the ratchet tree specified in the Welcome.

An AnnotatedWelcome can be generated by any party that knows the group's ratchet tree and the indices of the sender and joiner in the tree.

A partial client processes an AnnotatedWelcome in the following way:

1. Verify that the sender_membership_proof and joiner_membership_proof reference the same tree.

2. Join the group using the procedure defined in Section 12.4.3.1 of [RFC9420], with the following modifications:

* When verifying the signature on the GroupInfo object, the signature public key is taken from the LeafNode in the sender_membership_proof tree slice. The signer field of the group_info object MUST be equal to the leaf_index field of the sender_membership_proof.

* The "Verify the integrity of the ratchet tree" step is replaced with a check that the tree_hash in the GroupInfo matches the root tree hash produced by the membership proofs.

* The my_leaf value is taken from the the leaf_index field of the joiner_membership_proof, instead of found by searching the tree.

9. Joining via External Commit

A partial client cannot join via an external Commit, because partial clients cannot generate commits. A client could, however, join as a full client via an external commit, then transition to being a partial client by deleting its copy of the tree. This would still require the client to download and validate the tree, but would save the client the effort of maintaining their copy of the tree.

10. Annotated Commit

There are two main challenges for a partial client processing a Commit. First, the partial client cannot compute the resolution of the committer’s copath, so they cannot determine which of the HPKECiphertext objects in the UpdatePath they should decrypt to obtain a path secret. Second, the partial client cannot compute the updated tree hash, since they don’t have the full tree. An AnnotatedCommit provides these pieces of information, along with proof that the sender and receiver are both still in the group after the Commit.

```
struct {
    MLSMessage commit;
    optional<MembershipProof> sender_membership_proof;

    opaque tree_hash_after<V>;
    optional<uint32> resolution_index;

    MembershipProof sender_membership_proof_after;
    MembershipProof receiver_membership_proof_after;
} AnnotatedCommit;
```

The fields in the AnnotatedCommit have the following semantics:

commit: An MLSMessage containing PrivateMessage or PublicMessage with content_type commit.

sender_membership_proof: A membership proof for the sender of the Commit relative to the tree for the epoch in which the Commit is sent. This field MUST be present if the sender_type for the Commit is member, and otherwise MUST be absent.

tree_hash_after: The tree hash of the group’s ratchet tree after the Commit has been applied.

resolution_index: This field specifies which HPKECiphertext in the relevant UpdatePathNode the recipient should use. This field MUST be included if and only if the Commit has a path field populated.

sender_membership_proof_after: A membership proof for the sender of the Commit relative to the tree after the Commit has been applied.

receiver_membership_proof_after: A membership proof for the receiver of the Commit relative to the tree after the Commit has been applied.

An AnnotatedCommit can be generated by any party that knows the group’s ratchet tree (both before and after the Commit) and the indices of the sender and receiver in the tree. It is safe for the recipient to accept the tree_hash_after supplied by an unauthenticated party because the tree hash is authenticated by the confirmation_tag in the Commit.

A partial client processes an AnnotatedCommit in the following way:

1. Verify that the sender_membership_proof field, if present, is valid relative to the group’s current tree hash.

2. Verify that the sender_membership_proof_after and receiver_membership_proof_after reference the same tree, and that they are valid relative to tree_hash_after.

3. Process the Commit using the procedure defined in Section 12.4.2 of [RFC9420], with the following modifications:

* When validating a FramedContent with sender_type set to member, the sender_membership_proof field MUST be present, and the signature public key is taken from the LeafNode in the sender_membership_proof tree slice. The leaf_index field of the Sender object MUST be equal to the leaf_index field of the sender_membership_proof.

* If the sender_type is set to new_member_commit (the only other valid value), then the sender_membership_proof field MUST be absent, and the signature public key is looked up in the included Add proposal, as normal.

* The proposal list validation step is omitted, because a partial client doesn't have sufficient information to check all of the validation rules.

* When applying proposals, only the proposals that do not modify the tree are applied, in particular, PreSharedKey and GroupContextExtensions proposals.

* Likewise, the creation of the new ratchet tree is omitted.

* In processing the path value, if present, replace the path node decryption steps with the following steps:

  - Identify the committer's leaf index. For a member Commit, this is the leaf_index field of the sender_membership_proof. For a new_member_commit, this is the leaf_index field of the sender_membership_proof_after. Use this index and the receiver's leaf index to identify the lowest common ancestor. This is the node where the new path_secret will be inserted into the tree.

  - Determine the index update_path_index of the lowest common ancestor among the non-blank nodes in the committer's direct path, as provided in the sender_membership_proof_after field.

  - From the entry at index update_path_index of the nodes vector in the UpdatePath, select the HPKECiphertext at index resolution_index from the encrypted_path_secret.

  - Identify the next non-blank node in the recipient's direct path under the lowest common ancestor, using the direct path provided in the receiver_membership_proof_after field. Retrieve the private HPKE decryption key for this node.

  - Decrypt the encrypted path secret as normal, using the tree hash in the tree_hash_after field in the provisional GroupContext.

  - Derive the remaining path secrets corresponding to the non-blank nodes in the recipient's new direct path, as provided in the receiver_membership_proof_after field.

  - Define the commit_secret to be path_secret[n+1], as normal.

11. Application Messages

MLS clients can exchange messages by sending application data within the PrivateMessage framing. In a group where partial clients are present, these messages should be further encapsulated in a SenderAuthenticatedMessage, so that partial clients have the membership proof necessary to verify the sender's membership, the public key necessary to verify the message signature, and the credential necessary to verify the sender's identity.

As noted above, this can be accomplished either by the sender creating a SenderAuthenticatedMessage, or by the DS adding the relevant membership proof while the message is in transit.

Note that encapsulating a message as a SenderAuthenticatedMessage leaks information about the sender to the DS, including the sender's index in the tree and the sender's LeafNode. See Section 13.1 for more discussion of metadata privacy.

12. Operational Considerations

The major operational challenge in deploying Partial MLS is ensuring that partial clients receive the proper annotations to Welcome and Commit messages. As discussed in Section 4, this is up to the application. Since full clients don't need the annotations, applications will be more robust if they send annotations in a way that they can be cleanly ignored by full clients.

Partial MLS substantially reduces the amount of data required to join an MLS group, since it replaces the linear-scale ratchet tree with two log-scale membership proofs. Partial MLS does not address the potentially linear scaling of Commit messages; in fact, it makes Commits spartially bigger. There are other approaches to reducing Commit sizes, e.g., the SplitCommit approach in [I-D.mularczyk-mls-splitcommit]. These approaches can be cleanly integrated with Partial MLS via the AnnotatedCommit structure. Table 1 summarizes the scaling of the amount of data that a client needs to download in order to perform various MLS operations. Sending a Commit requires linear-scale work in any case.

Operation	RFC MLS	Partial MLS	Split Commits	Partial + Split
Join	O(N)	O(log N)	O(N)	O(log N)
Process Commit	O(N)	O(N)	O(log N)	O(log N)

Table 1: Download scaling under protocol variations

13. Security Considerations

The MLS protocol in [RFC9420] has a number of security analyses attached. To describe the security of Partial MLS and how it relates to the security of full MLS we summarize the following main high-level guarantees of MLS as follows:

* *Membership Agreement*: If a client B has a local group state for group G in epoch N, and it receives (and accepts) an application message from a sender A for group G in epoch N, then A must be a member of G in epoch N at B, and if A is honest, then A and B agree on the full membership of the group G in epoch N.

* *Member Identity Authentication*: If a client B has a local group state for group G in epoch N, and B believes that A is a member of G in epoch N, and that A is linked to a user identity U, then either the signature key of U' s credential is compromised, or A belongs to U.

* *Group Key Secrecy*: If B has a local group state for group G in epoch N with group key K (init secret), then K can only be known to members of G in epoch N. That is, if the attacker knows K, then one of the signature or decryption keys corresponding to one of the leaves of the tree stored at B for G in epoch N must be compromised. To obtain these properties, each member in MLS verifies a number of signatures and MACs, and seeks to preserve the TreeKEM Tree Invariants:

* *Public Key Tree Invariant*: At each node of the tree at a member B, the public key, if set, was set by one of the members currently underneath that node

* *Path Secret Invariant*: At each node, the path secret stored at a member B, if set, was created by one of the members currently underneath that node

As a corollary of Group Key Secrecy, we also obtain authentication and confidentiality guarantees for application messages sent and received within a group.

To verify the security guarantees provided to partial clients, a new security analysis was needed. We have analyzed the security of the protocol using two verification tools ProVerif and F*. The security analysis, and design of the security mechanisms, are inspired by work from Alwen et al. [AHKM22].

Partial MLS preserves the invariants above and thereby all the security goals of MLS continue to hold at full members. However, a partial member may not know the identities of all other members in the group, and it may only discover these identities on-demand. Consequently, the Member Identity Authentication guarantee is weaker on partial clients. Furthermore, since partial members do not store the MLS tree, membership agreement only holds for the hash of the MLS tree:

* *Partial Membership Agreement*: If a partial client B has a local group state for group G in epoch N, and it receives (and accepts) an application message from a sender A for group G in epoch N, then A must be a member of G in epoch N at B, and if A is honest, then A and B agree on the GroupContext of the group G in epoch N.

* *Partial Member Identity Authentication*: If a partial client B has a local group state for group G in epoch N, and B has verified A's membership proof in G, and A is linked to a user identity U, then either the signature key of U's credential is compromised, or A belongs to U.

* *Partial Group Key Secrecy*: If a partial client B has a local group state for group G in epoch N with group key K (init secret), and if the tree hash at B corresponds to a full tree, then K can only be known to members at the leaves of this tree. That is, if the attacker knows K, then the signature or decryption keys at one of the leaves must have been compromised.

Note that the Partial Membership Agreement property holds irrespective of whether B has verified a membership proof from A. The membership proofs in this protocol are thus more about providing precise source authentication within the group, rather than simply proving membership in the group. Simply knowing the group's symmetric secrets suffices for the latter.

Another technical caveat is that since partial members do not have the full tree, they cannot validate the uniqueness of all HPKE and signature keys in the tree, as required by RFC MLS. The exact

security implications of removing this uniqueness check is not clear but is not expected to be significant. In a group where full clients are honest, there is no practical difference, since a full client will verify that all of the required uniqness properties hold before issuing a Commit. The main risk is that a malicious full client could cause a partial client to accept a tree hash representing a tree with duplicate keys.

13.1. Metadata Privacy

The protocol described in this document assumes that the DS is trusted to know information about the group's ratchet tree. The scenario described in Section 4 assumes that the DS is maintaining a view of the ratchet tree and distributing appropriate portions of it to clients. In fact, if the DS is to generate membership proofs to accompany PrivateMessage messages, then it will need to know the index of the sender in the tree, information that is normally encrypted as part of the SenderData.

It is possible to operate this protocol in a more restrictive mode, where Commits are sent as PrivateMessage objects and the committer generates the required annotations for any partial clients in the group. However, because there is no confidentiality protection for the annotations, they will leak information to the DS about the ratchet tree.

Fixing this leakage would require changes to logic at the committer and partial clients. The annotations attached to a Welcome message could be sent as GroupInfo extensions; effectively a partial version of the ratchet_tree extension. The annotations attached to a Commit could be moved inside the PrivateMessage content, and the receiver signature validation logic updated to use the public key in the attached membership proof to validate the message signature.

Thus, while a more metadata-private mode could be added to this protocol, it has been omitted for now in the interest of avoiding changes to full endpoints.

14. IANA Considerations

This document makes no request of IANA.

15. References

15.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[RFC9420] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", RFC 9420, DOI 10.17487/RFC9420, July 2023, <https://www.rfc-editor.org/rfc/rfc9420>.

15.2. Informative References

[AHKM22] Alwen, J., Hartmann, D., Kiltz, E., and M. Mularczyk, "Server-Aided Continuous Group Key Agreement", ACM, Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security pp. 69-82, DOI 10.1145/3548606.3560632, November 2022, <https://doi.org/10.1145/3548606.3560632>.

[I-D.ietf-moq-transport] Nandakumar, S., Vasiliev, V., Swett, I., and A. Frindell, "Media over QUIC Transport", Work in Progress, Internet-Draft, draft-ietf-moq-transport-17, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-moq-transport-17>.

[I-D.mularczyk-mls-splitcommit] Jol and M. Mularczyk, "MLS Split Commits", Work in Progress, Internet-Draft, draft-mularczyk-mls-splitcommit-00, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-mularczyk-mls-splitcommit-00>.

Appendix A. Test Vectors

This section provides a set of test vectors that implementations can use to verify that they correctly implement Partial MLS. In addition to test vectors for joining and processing commits as a partial client, this section includes test vectors for membership proofs, partial tree operations, sender-authenticated messages, and the syntax of the new structures defined in this document.

The vectors included in this document cover the MTI MLS ciphersuite, MLS_128_DHKEMX25519_AES128GCM_SHA256_Ed25519. Full test vectors are available in the GitHub repository for this specification: https://github.com/mlswg/mls-partial/tree/main/test-vectors (https://github.com/mlswg/mls-partial/tree/main/test-vectors).

Most values are either numeric values or byte strings. Numeric values are represented as hex values, prefixed with 0x. Byte strings are represented in hex encoding. Descriptive fields, such as message types, are represented as strings.

Line breaks and whitespace within values are inserted to conform to the width requirements of the RFC format. They should be removed before use.

A.1. Membership Proofs

These vectors exercise the construction and encoding of MembershipProof objects. For each case, we provide:

* cipher_suite: The MLS ciphersuite.

* tree_hash: The root tree hash of the ratchet tree.

* proofs: A list of membership proofs.

```
   cipher_suite: 0x0001
   tree_hash: af2e61d379b5838228ee68aec6b4a733e2a732844b749ceef618b8712f659a8f
   proofs:
     -
       00000000000000002412d0101201a28e7c83d94808952f4c93492fc1eff3d7ede
       6d4d8652c862e21c8f8c6bfe0a20eaa4536432d5d0e2b100d94e76f4c427238c
       e4d1c66635ebb23bc0e78a128e9000012072a1e66a53e5df453416d4076be972
       ec1eae4af1af8e677aef59cf59b686a35f0200011c000100029a9a0003000500
       073a3a0006000400080009000aeaea6a6a04caca1a1a021a1a0c00010002fe00
       babacacaff000320ad7c01f29bc6916d7c4451cf195e554952562962a566458c
       14ef6b19375b5f93071a1a044239abd64040a5f834707f202b7af4bc190802d2
       dc66a5c46f9ec066421db3f4326848c6ab2f294e988621489c7d2cbec421bafd
       7f5607adc9dac36edfbb89ffc5bda7d70b0001022086ddb23caf21f4793ce157
       f29a0a3de1a81036fce607d1164efdb26da7398036000021207b89c575d1019d
       20742fc67a7ec831bd707a5827dfba14416daf96ca92ed236d
     -
       0000000100000002411701012 0cb907f82e0a7923f7a505a49ee9e19d237cbf2
       6ce4485112f83d92acf39d722d20c95b4791c9b169cfd217b3db4368d70800a2
       851e0717f70650a63d9018cfc1d4000120c2886ff8881eab6f3ade3df94c2f72
       316255f0ea338ef633031c6b1b9300860a0200011a0001000200035a5a000500
       07000600048a8aeaea00080009000a041a1acaca02eaea0a00010002fe008a8a
       ff000100000000000000000ffffffffffffffff061a1a03cfd06b40401f04051c
       dc088d473a23313409e0ba6ca7fed554097c0936f1489e67b9c74993b063ce97
       cc62d6286e78d827d1a5a5855af12e7a70690c23744da47f7712120801022086
       ddb23caf21f4793ce157f29a0a3de1a81036fce607d1164efdb26da739803600
       00212085283300da17fbc5880f483b593089103b18b1d3c4c5b4c359158ce9e0
       2085c2

   cipher_suite: 0x0001
   tree_hash: 12b5599a8fdb272460f91ad2445790ccb8269138b9ac51da7b7e70c7ebc5edc8
   proofs:
     -
       00000000000000044169010120e330e4c8231f96e35d800360d6f0a80073299c
       11a9d3a182bb2fc798e3bc2d512062035c6d4d91abb7c272ed79d03ea4141cc1
       2b7cd1d58ceff3c9d3309e39737e000120e5923186b07cd29fecdfbfec95ac0a
       535423d5890f2c6499b0b6b80e549d54db020001187a7a1a1a00010002000300
       0500070006000400080009000a049a9acaca02eaea0a00010002fe00ff000a0a
       0320438b547576c4c5026dd11ace02fb75dceda54df81786b2c63aeb5f53da72
       093804caca012e40404f0c51bf2da1ece7fcde8ee283b571a5665684e746c37f
       b9c2a9de7501a8f34a6e58e08b4022895be7959cad8393d3ec78227944a44b5c
       923a081bf38128b302010220f455b3651572b742c36ba3eb582c4d8d440467ec
       b2c4e03406127b40ad3aa26020021ef39134951ce83c11c1b8ecc1bc4a9f5c5f
       1606ca7fabe90128ac4c36b6b500010220a9f7283bc748e662cefda8d1d330c8
       c9a1067cbce1632a4388fab232f31704700000404220cc3943c3a57c354f1de8
       4107af098c998c80a8ca3f98397c702645d7d3ecb3f820e387830f39d1eebc2b
       d4e75350fbcc1e5dc67a053cd03ff745fe0cad6f15be69
     -
       00000002000000044176010 12079d678865eb29b467929327149d5eb49838338
```

```
      809b842a2d2bf309dd49d8f52f20551324cdfd59ca1aeda2f52c91508f42526e
      eea68dffad2481e21f8380c1098b000120b5e2cdcf69541b1adfcdf0d8690bb2
      09bc1d4c3f5fb0ca86434c5be374532c970200011800017a7a00020003000500
      071a1a000600040008000900 0a04babadada027a7a0a8a8a00010002fe00ff00
      03203e97dfb02ee292a21f095c22f03e51d2bf2125891740b74eacb5d90ec9ce
      d45d11dada0e4673161c625e4941a520f03b3e064040486851d2ee5e1a8b0d0b
      fabb7f7da8c81e6c3b00bc8009225b99f9971e205a1a695c78400e8e8c05d93c
      ae692967d9d10e3ee186a963a821cdd2bffbecd340040102207a2176979bce8d
      7df4606425358a20cf1edd44b68567769368e05ff5d8d5404620b0427dcdeded
      feccfe48c0421addf10170bdb97ccc682e7860718f5761d9f36100010220a9f7
      283bc748e662cefda8d1d330c8c9a1067cbce1632a4388fab232f31704700000
      404220e70ed34565006bce39a9faa965856edfb350e618d80023abedac07c6fa
      69e303209e660559c3042bf976297982887832806306558aa32eded402c24481
      c0b6c097
    -
      0000000300000004416a0101207a300aa9dadf5e466686c474d9fb632ce80212
      0e5187faf858d942a300a6684d2022cefca1354d50979b23d0dfeb061768c5cc
      f091c314d8a253541273733aab9900012069208b9da0a0db8f589ae336e53086
      9e106854bc5d743caa214249fb9e7a57ff0200011c0001000200030005000078a
      8a000600041a1a00080009000aaaaa9a9a044a4a6a6a02dada0c5a5a00010002
      fe00ff001a1a010000000000000000ffffffffffffffff104a4a0d575792aabf
      6f4304d4e5240ed040407fc9d720bd5c240d627f50e55dcf9a6d404b43620b40
      e9b2ce640b1f87f7f064f8b3d5463264cdd042032165a285b06dd4bcd77f839b
      c7bb9601a6a81adc13020102207a2176979bce8d7df4606425358a20cf1edd44
      b68567769368e05ff5d8d5404620b0427dcdededfeccfe48c0421addf10170bd
      b97ccc682e7860718f5761d9f36100010220a9f7283bc748e662cefda8d1d330
      c8c9a1067cbce1632a4388fab232f31704700000 4042207b46ee699a0da207c9
      406ff317ccf9eca7cc18ee6dba2320a416fd5aa6c6340b209e660559c3042bf9
      76297982887832806306558aa32eded402c24481c0b6c097

  cipher_suite: 0x0001
  tree_hash: a60690be6de91d245ec8f8b3103b8714bf7f1eca1b31185e6e92616142017eb6
  proofs:
    -
      0000000000000000841b601012020af6a8619106a7e1b727aa9b7cbf300b845bf
      9c818e35899d2528e6663f1f60202a1b59be4c45e035e192130534c17881d86b
      c06d215a2f9081fc71aa3450bcfd000120f06e197bb4952035364d00dfe65a24
      82e403f3399e640d321ce7775a3fbb755d0200011e000100028a8a6a6ababa4a
      4a000300050007000600040008000 9caca000a04cacaeaea02eaea0a00010002
      fe00dadaff000320633fb04c9ce9d507d0472d434be015267627c1bdda77e058
      39365fe93e9236f906eaea03dd22314040b4b6941acc6ed8dec777362f6b85c5
      70dae41d5c5ac6366c71928ebf871b7735091afa61ad7807509b7f6822eafd28
      6f4b3538e0d85839b2924debd105d161080102206d956e986a01a81e2feccf8e
      fa1fc696eca43b027790d02696b4772920849707207 9436c917b632ef8c92d2f
      f39ace503d5bef4c051f602cc9136b072b663fe78b0001022063abff459703bc
      15753a7279ef3ca6941884f5c36d8a6f9926227fcabf2b5e3c20a08451842dc2
      dad9148377abb1d9a17fb8e5240d2a178b54b2cd8371c41f477a000102209c0f
      6c61337ba2724854d8bb7db1c7b0428a474a657d6aa6dc547c805aa4d3560000
```

```
      406320c8b74840869c0de6ab59351933b3c98d988d59d813f811f2215a97581e
      e73b5720214c324eb39cecff629a1ad2e18f2c3a2af8dee01a2cf3f0512fa3b7
      fcaed39f203b9909ce1fb47f1f8583d3749bed6bd5d1dde6355612429c69cbf4
      b613e87aa9
    -
      00000004000000841bc010120c1fabd950a61c0dc2c6e812779fd7e0af8a386
      e0f4a15e788c04f6c7a382c3152072ba8ce72f492dde95f64222a671af1615c6
      77fcff561220fe19e565deec4210000120d59205a6ed7163eaea5d629425d332
      362eea3a96366c82c5b5e6e01a65a942b5020001187a7a00010002000300052a
      2a000700060004000800090000a041a1adada029a9a0a00019a9a0002fe00ff00
      0320cbcff5c474a529acdceacf706146b87e579fcf0732b8ab7ca672447ce6b9
      1a17121a1a0f52a383c49622b5752be547259829bb404079c269c71b1dfbbe1a
      5a6847d0593c9ffc5a0116802305e8c55fda6e80d48a20d4b8df3042e195c2ab
      0c2182ee96b320fd68a958a5a1b2ee74124a11ce0c0f06010220eb4d45c4e188
      5540cbd9d3dcb613a32429d8f9eb7864b0029da0b0460beac94e201536f71515
      135c3030c2a73affcce5bdaeab9857546f1847ead33ac1c3b332b900010220e3
      792af43b2029617b886a9fb5d80c2d4926899c3c5536155a5e0fc37af3d90820
      f3809f6145028bde20fa9866f9e709a10ec8c69ba79600c8239ff6341ceb8cb8
      000102209c0f6c61337ba2724854d8bb7db1c7b0428a474a657d6aa6dc547c80
      5aa4d3560000406320757d1b5dbe69bd5cac07347e5f1adad78d42e8142e379c
      a33b2e2def7290210c2096b2310a2906457e62c6f6b27c19e2b4ea03fa67148a
      d6b3cf96593a34e3bd2b200fd29532e0530c35b1fab33581dea89ce4b8df3a55
      bf28a452d107b9d820769a
    -
      00000007000000841b2010120abf22f1cf3409ad5e836c526a0ce44dd570f3b
      17b314935ba2c1824705591212202247 85a7d77c395fe930b5c25f9269263173
      b9e6073eb7d724d386343d33d3500001208091bb121591bbb3b9e41cc552360b
      eb0dedf3038f3c3060263d1e3bfb6bd9f30200011e000100020003eaea9a9a00
      0500070006000400080009000a3a3ababadada04caca0a0a02baba0cbaba0001
      2a2a0002fe00ff0001000000000000000000ffffffffffffffff11caca0ec64cbe
      2565935a1c353ccddd4de34040cc086f140b00a20cdf6ecd6c84ecbaa0a3a0b5
      d1d7efdbf0af9d3ed77aae9c85863fdb2329cc8bf649fba01b7bb9a5241a4efe
      6a55d10e0c800e59a4a94af701010220f1bc2c408ef2321aa9004f0f64e01d30
      784019211bdededd9dcf7e2c25bf405120a9cf2cf3f23eb9605b1f4dd9c4d40c
      d1b78cc29733b5664f550275ea91796ec100010220e3792af43b2029617b886a
      9fb5d80c2d4926899c3c5536155a5e0fc37af3d90820f3809f6145028bde20fa
      9866f9e709a10ec8c69ba79600c8239ff6341ceb8cb8000102209c0f6c61337b
      a2724854d8bb7db1c7b0428a474a657d6aa6dc547c805aa4d356000040632027
      378fedbb010a6aa88d3aeb28f69f9010ddb95580850c36c824983ea334f81120
      ee240a956d3a2239fe7eb45871e42bb9553fa726424d96306ed7965a4a0dbb7d
      200fd29532e0530c35b1fab33581dea89ce4b8df3a55bf28a452d107b9d82076
      9a
```

```
   cipher_suite: 0x0001
   tree_hash: 0df49398c7800aaffc30251a55f67c06b359c1837887c1f6d6da75821873421e
   proofs:
     -
       00000000000000204237010120c36c2c859f0890a483c44eac3411ac9b879b43
       73fd90a116156543e618aeba1720d33251c672a387ff76717f5795d05fb8d9cf
       0450aee5b32dc0714addd7ac9bc50001203c7917d8b9ef23e338979bb35e6347
       b6893630ac0fb57859c6924f5a88cf6a1c020001160001000200036a6a000500
       0700060004000800090000a04baba9a9a025a5a0a00010002fe00ff002a2a0320
       6d40c5f79db4f7af6c84091f05f09dcdc3bb69e77b2d9a32e92de3b5966518b6
       059a9a02078b40401ed441b56dcfc24a3b79d01ec24b7c7603066e7a5a92795f
       e372d4c17c6b9c2527772cdc4448d3022177250ba931f63fecb3af145ccbaa6f
       29d4da89adaf0f090102203e03b835edc3816f80776cfa3c2dc2909bb10c4dab
       c17379e7a6d68faff04b7f209adae2f21c9fa67167cc0a5db8cd1540a19d8293
       32ad36cc828492ffa2d7200a000102200a2f20e59688d3b653064241293f9e1b
       ca47555341036b866f2ed77334f49d4d201540aded33bc657bcf3645d8c3e1c7
       e994a41390770b18fd20febd1995354a9c000102202428c7094d2dc227cb5a80
       e75cdd4255ba05a99fdec66506c3cb7612a743c11320563eadd6c3858c366dbc
       2a8106efd1a176757f2020e99a82913ebad252694a3500010220afa8581a8dec
       58d4ce7c076f4fa347168a6d2f8c38dc728ac941dd0229e2067a2069be6519f3
       5fb6614e850a51aa3174dfb466ae78226b0137f1b1164da3d1a0a90001022095
       626b26216455b579b7050fd538efa676c1f3b10b50f5a853c2c9101ae8c45200
       0040a520ff717486f994b943dd27694ec95c354172b9487ca16c9f065d25c8aa
       7c22ec74200dbe544ae3382c3a621509108114a149a65d1465a037d99e16db62
       fa5531706b20acefa0ff950f86c83d0f897db068c0acb544865010c8115597bd
       07a6f4e0697c20ab3a8a890f5a68a88c975071505bceda51c6999d02d78bc2f6
       51b038f1727871209ff36c05e51a6a848ddb6192ed8f1d529873cb064498c0e0
       7bff39f4e0031da0
     -
       00000010000000020423d010120d4cf9edf116c5a861c33209ee8fdcec7d2b10d
       b36159f0a03011ce222c57763120f91090f471a0fc126dacb69360b414da3690
       4ce64a39498846c7df0adda6fa3a000120ef1c5c52f234f59070ecc3f8cef845
       a4fe6e52c7fd4fc0cc468a7c841a559b5a020001163a3a000100020003000500
       0700060004000800090000a044a4a5a5a02caca0a000100029a9afe00ff000320
       53bac0e284ea350f8a832bab95732c80128fd2addf32daca602fdbd7a6e7c62f
       0b4a4a080fac4ce74324b7af4040cc5ce08cdc91338c51170c169fcc7ea81c5f
       8cee803a1a1ff1de277bea295d34a5343b82712f02c1a2a680991cf373eeaf70
       3956ffd813e0092bf02a12fbf20b01022006bc1a624723bd9dd5135d8844fa0d
       90565bf8a4aebc0519388505d0b5df484120b81e6360af397fb28610fc3655ad
       7bb84662c66bfef878c2ff69ca29604dc5f70001022084eb92f3fa27e7a6a2af
       235ffe8746690635c477e9b09f0c1d1d0e42506b706e207c4d3916f6330a990f
       fce0c599d452e540ddb8d5d2e967d7750255533a904c0900010220a6c3b49792
       7d5aaee67991eb370cdcef8ae60617d7b60abfd07e8dbd00e6e70e203ec2537d
       7f941ca5c6e12ec3fff5e93740f82857e277a6e909e6635569372a1d00010220
       06f434ba132b8e16d4d58e81912681071e8969b01a7887f8ddfacb0db72bdb35
       20a904e70ffab86a117321e8524812aa4377b3f0081f237942b9a4f2b1b16e2c
       8c0001022095626b26216455b579b7050fd538efa676c1f3b10b50f5a853c2c9
       101ae8c452000040a520bbcce2df32a7e4d0ae8a036c495d09a10093caae6d48
```

```
      db1e5139b7a612005da320e0be801af538522aab4111b080e19edccdccb05408
      24bd5990dfe4d0a19d19e020ed533bddc13912621cf7438fdd3d7c9ec974fd62
      45732a56566f164d5a87dd8d200dc44fc0a3935e9747b5eedb6df99d8089975e
      559e746580cf6d832ed1c020b120dab04be145ce862921c6d7193195fe809655
      e5ecb541be57ff334bbf9eb0e61d
    -
      0000001f000000204228010120f1105bb8518b3be94cb57e10ccd34223ecd780
      d6846fd07b88c89485a6c3f07d20d05fe820bbe7e965a86f6f100357b433f5e3
      e8aa18f84d90f6b296753ee47f46000120dd8a47206f79b8d28a63b3d8901424
      79e8aafd27478d30c9c7f0910798e5d5850200011600010002000300050007000
      06000400089a9a0009000a043a3acaca023a3a0a00010002fe00cacaff000100
      00000000000000ffffffffffffffff07caca0461813b66404053c3efb158e59b
      c84eef3ce500370f030114cb5a4ac4e7eabe835e386a223f41b49251eb667a02
      0ca89c0bc5d87e9185575173350c0c42c3b4a2ac0a27ed9a01010220a93f1e7d
      ffb17ff3295bdee652cb7f156c95a019beda8be6b85f764328c72b6120dbd34e
      37176d959c5290aedc1f1eef8b8075b6d8b76e6c0c73336fe69a24d20a000102
      205f0e2eafb8d49f293765284092bffa156cf380a45a7a5fa24b937f15a69322
      4f20f44b3a43d6a55eeed38f77db395569a625c3382266d966b4f52c8faf4b33
      35a7000102202ff338a32ca5a892890bd154f013fddf4522fc6de3b5cdd1c490
      39d91ecbb906209897cfa22fce229469ce6e56e7378e292a36643b10ff06bcd4
      fe61b0a6e074540001022006f434ba132b8e16d4d58e81912681071e8969b01a
      7887f8ddfacb0db72bdb3520a904e70ffab86a117321e8524812aa4377b3f008
      1f237942b9a4f2b1b16e2c8c0001022095626b26216455b579b7050fd538efa6
      76c1f3b10b50f5a853c2c9101ae8c452000040a5201f50ef3d6192c2b6fe7253
      6db3e1faf8edf4b06a321e20004fbe83eb81e1bfa1201c5f55865f82adf4eefe
      d83cb5c8c73a0c03cc20ca235d4bfea0599ac7f5143d201f0de60f83fa1e5d12
      aa02ad5a2b2cd991a8f83b90f88c90445e62defe4130f320b62601587e8938dc
      824ed728bca5a368398f8d243f2e016882e3776e4343913e20dab04be145ce86
      2921c6d7193195fe809655e5ecb541be57ff334bbf9eb0e61d

  cipher_suite: 0x0001
  tree_hash: 57524a39798ed441e1fc30500e06496c59b4761e0e1af04db44e3600e77f7395
  proofs:
    -
      0000000000000000841b1010120c03447385bc538a758f6e5e8441069cfac168f
      047e4fa1defcb36524fd08b87f20ff48aae39166a4825c17e991e1704ee12ce2
      ec572317a6fe9c6023f5c7cdc08d000120309648af5579dd228ea269a027b392
      e21bc6c20609213fbc5bd2e4c52e179521020001166a6a000100020003000500
      0700060004000800090000a041a1a7a7a02aaaa0a00010002fe00ff00aaaa0320
      598845933e05f119b9c1324ff8a868549b61189899b222646bf345a4f0143faa
      091a1a06aa88e105cab640408830aff77c35c68bbda3ed323f74e1cfd59db5de
      a0c5c0a4abda8ad0a9d06ba7ec1cee85703ad14de813a067c55ea2d7864ec49e
      c5a8241a826990ed3de4080e010220e1871d1f1ab8b5eebaa46425514785de38
      48c6b12b5659cc586b7ff209ead73d20e555cfa3cf16a1a845d35c665b5e33e3
      ad52183dd58b75421b2f9811a1fdbe7600010220bd0a65cea15a0d9b37a7107a
      43ac11cc5cdf9ccee177d15aca834ef47a8aca6320f581eb8c6c8e1af54f4868
      fe0d2ee6cb3cf556d33c6b2c8707fdd575949937c600010220d963c3d217d7e6
      573b0ddb011a2992b414f18f7fac2cf0875ab56398c22b6a760000406320788d
```

```
      9c69179eb00281a8191d48db2d9ed6ef64f0e861cfe82e40dda75ef38d8e203f
      b03a0dd2a3fa7cba79b67cb65c84d77b7abeb81d08e9f50661a6c117f6dfbb20
      0dbe1fdd5aedb29a5430151a99a74b75eada0404bd0c11ab68d960c32dc29e37
    -
      0000000400000000841b2010120413a88e151ab8a7d0e67da7b24b3cd1a28e719
      de844cf8f61879ae7d4b4d640a20cb4aed0276999a2a861870b4c6fa0fc74e13
      e295cddb53ce9663c02e262f1061000120bcea448954535048b7c21ab75eb60c
      d9d35fc38110403ab2a9aeba8dec8c5bac0200011a3a3a00011a1a0002000300
      0500070006000400080009000a4a4a04eaea9a9a026a6a0c5a5a00010002fe00
      4a4aff000320bec8c716d15bf0e28e7f72be54a300a05c07e570e668882c2eb1
      9b33818b880b049a9a01a1404078875601f95b8eba8053a052fc6ec2acb1ffe2
      0211df98a7e3d3756dad49d2e9fe627d6016b84fc75a6ec082d23ac3be14554c
      12c52d86de6935c1a4ff4ad3090102208636119079 4ba624dd524a355ddb6f54
      a861675a0edb87966fe33a29d6ccf83520c9858e41c240a6372c44ebf4dc6f47
      51e3c5eb9bb888c9cf23aee8e448e1c8b900010220fa9afd34ee44d67cf62b7b
      afa6d7d794ccf5064d5327913460d255c97105664d20f9ad8f3f8cdaa409419a
      647f63d965528024745b977cf9658fe7de6e1aa4245b00010220d963c3d217d7
      e6573b0ddb011a2992b414f18f7fac2cf0875ab56398c22b6a7600004063205e
      e87e71b72002c8befceb043e1b4177196cb6d041a2c28ce1082eca32e2c94520
      9e00e4a9e96809453ef3ac9ee86ccbb274d994f0a3b711cd5e06056dae5094ed
      20b971bc78225999bf56a393da4b9856a7170aa9152425191cb972d274466d7d
      67
    -
      0000000700000000841ab010120f4d22e604039caadc6ca61324501b32373d917
      4f144e7efa9e5820f5b528e95820150d93fe718811668d02f23d25f70f9d6749
      454aa911361ef3720e0bbb3c730500012040e165431d54b1142f9e928e4db11b
      c20e85ae5cea9456f2cd1721e52d6bb3fd0200011c000100020003caca000500
      0700060004aaaa00089a9aeaea0009000a02caca020a0a0a00010002dadafe00
      ff000100000000000000000fffffffffffffff10caca0d1276d5a047cc0817e2
      d6642e2b40403fbb0bdb551f289dda27955880cb79c84c276a1cf1a3e5adb950
      6c7ad5ee21ec15b82e4b7b8d523b81fad9de3fb5cfe1602abf41b25f054afb4e
      bb79a8b5ae0a010220cbddecc3a44c1ce6ef129c5d48cd6407df6d887786c5be
      d449c465b2723c84342023972e867d43baa13ba9eecff7b35ca8235b3a98d5a6
      2afbb39b9dcf21c103c900010220fa9afd34ee44d67cf62b7bafa6d7d794ccf5
      064d5327913460d255c97105664d20f9ad8f3f8cdaa409419a647f63d9655280
      24745b977cf9658fe7de6e1aa4245b00010220d963c3d217d7e6573b0ddb011a
      2992b414f18f7fac2cf0875ab56398c22b6a760000406320c5df1e7ac3186fbe
      a4ba6e1cc6190d898ac5b296db87befb8c356553f999e6c420b44cf23db8c781
      1ab10423353fb66887f5abb093590aac55b7af61a6f2d1131020b971bc782259
      99bf56a393da4b9856a7170aa9152425191cb972d274466d7d67

  cipher_suite: 0x0001
  tree_hash: b11f7c39861824542544f8daae4f2f3e0c9874ece6adee77a6b14cee45088ee1
  proofs:
    -
      0000000000000008412d0101209d43ce5de1a45e708aef6c7c0c1b120492f8cf
      18a5c4798042b543a63036f64020eb7320019c41b32f8261ae0fbbfd4b1659ce
      71d1477d700565e1efca8ff4e9590001207f129dd4b46dad54487e908aad183c
```

```
      8e0827158bd063a1eb90236156d2bdd3f902000116000100020003000500076a
      6a000600040008000900a049a9a4a4a027a7a0c00010002fe00dada3a3aff00
      03204fe938a61e88df969297ebb39905ae5b547b3221c4adbd9c2df59def3f74
      609a0b4a4a08daba9c58fdca99a240408d6a0d4480a33582eb098c90d7149912
      d1d62b738bc5263712e266333e3f873866b5526ac4df79948f6203fa54f76703
      def2e0b7a0382cd5f382198e406a01060000001022066f0e92224a1cabeda5d7b
      8263831b8dfe3bf93ca0870eeefc5993616a7adb700000406320a90d4563c6a0
      ae0417ab3110f1ba6859283346595477420 1b0a69e8c457dc6ad20c0d2b83fa7
      6a6a182e97682d717acc9427d8e7e4dbaee5df157b72fa332732a520cc9475b5
      4ab0db054de1b3324f991956b1ed84662110a5659473bc8af32d0013
    -
      00000005000000084 1c10101202ef6fe280d8db111d10004f2dabb5f3b92604c
      4f2dc16dae5620daf139e6fa4e20687786292743847b27aea13d3364cc499d9b
      4b968267c87561cd8a319c7610fe000120ad7e4636852270777c0bdcc6b921b2
      02308d15baae3d9427f1fb3a399f19f8fb0200011e00010a0a00020003000500
      07000600041a1acaca00087a7a0009dada000a04eaea4a4a02baba0a00010002
      fe00ff00aaaa0320d7e181dadcf7beb20e93404bb05d2a1e5c979f5fdcfbef93
      5bb629e29e645754114a4a0e58e4576ea1696306e3b1b3a0ec54404061d2bb40
      4bf7e721513de0e0d3b9c6e872ed3bfb3aa9236a278f3c0cd0fa818232f1c677
      2a267944f73386eb670cfaba71f340cc645e60fa6fc21fc37bb5600b01022029
      6b0edc627e8e0ed97c39c63228d88e7bc14701718fe73cdd9c4f10bc29011020
      e13fcd8ea180af77268010c55b7a2465f679bd8636170c901ab271b0ed6904d1
      00010220abaf724a22813c349f73eb8d65d1d2e8f1c8fd12ced328f7d6eee1d3
      f8c7a22a20d986e9733197f76b16c149790da8d3aa8ce0d0c10ec07b5c05d10b
      afdddf46680001022066f0e92224a1cabeda5d7b8263831b8dfe3bf93ca0870e
      eefc5993616a7adb700000406320618cbdc4c471593366ce37d43a9500e3255d
      5e4162c821f4cd386a769300e48720a8a9768b204846471153e956520089971e
      1390464947c2e8f5ec90bc92ca3f062031c4741c7a0cad3826984f29ee5683fe
      001458b83cdd41a065a56319bd023fdf
    -
      00000007000000084 1a701012073dae92a3bdf3423a2545e15ac2cb5d4b1b8c6
      a9b9752253e02d1e567ea6e66120ca06979f99cd7b273999fa39a20366eb7312
      44cf4b38b9e6a0a4a6faf52c1f370001207d205f6e0c5eb4d4337fcf14271e7e
      b95a92f757d64845f1dc2d745e70a7fe000200011600010002000 3baba000500
      07000600040008000900a02caca02eaea0a00010002fe004a4aff0001000000
      0000000000ffffffffffffffff12caca0f905d7b10f2f07c66d987334cf42b41
      40404164717a61deb7dbf00fe3701281ed0faf2530ff8314c975b1dea2aac4b9
      e107ab2994f884d34116758061697e4e1cf6c831ddd4a4fa4ee5aadc58ecc77a
      f00a010220dfcc93d78a2b1038410b8ae7d2df8896bee1c6475c8cf42ac2323b
      d89699f0632071a5fe7002a85cbf535bb1d0ba9ea12235c215850633a587b1e9
      ae772442eb4200010220abaf724a22813c349f73eb8d65d1d2e8f1c8fd12ced3
      28f7d6eee1d3f8c7a22a20d986e9733197f76b16c149790da8d3aa8ce0d0c10e
      c07b5c05d10bafdddf46680001022066f0e92224a1cabeda5d7b8263831b8dfe
      3bf93ca0870eeefc5993616a7adb700000406320ba45a7c3e98ed62419ba2418
      60fd61068012147a7ae10d9836a52540975c10c920b9111ca283f06ddfd0c632
      bcbcf1c2189dd8d36023b3f2da394fce289e77d8a52031c4741c7a0cad382698
      4f29ee5683fe001458b83cdd41a065a56319bd023fdf
```

```
   cipher_suite: 0x0001
   tree_hash: f2c886ee356436afb51781989db8da4e44aa0a515f1febfa04f43613a7df96f6
   proofs:
     -
       00000000000000841b70101204fa3c5cb9746a4792d70b1123c3ac3925483c5
       30e6afbe023e7945315e3b9c6920c77eeccc3ae46a63a5039b3087f497693f32
       487ab0685d9ab56bcb8039729392000120b7acdfbfed25e6aa59eb7bd8f5aec2
       05f7503b16c15d44613d6f8dc4019b7eb10200011800010002000300500079a
       9a000600040008000900 0a2a2a045a5a6a6a028a8a0a00010002fe00ff00baba
       03208bf2dde271940cc5c706fe7c503f10dbf2e551c0d3fb59cf69b9a42e108f
       dd8a095a5a06d2fa2bd5eba240404e3f24259ba97838a75e0ece24348d5b9b66
       33c63c921019160ce7fc0486766d4ad49f063973b42edc8c8f966cca84b576dd
       5ef18394d3072b1ae6b446cb3c000102205bfda21818c70c1ba03a76ea0d9902
       ddb6d3e25c1a4177b138d7082ecca54a1220428784c1f832c8a58c5b53f26f20
       dd27d187defb1072bec96568bb420e1fb821000102208527bdc96b6eab6a1798
       1544103a4b9ca8456430884cfbd1a1ab7ca5ea973e612022b1f446cf92472016
       da8f296cecc7362cfedf10853a52d6a4a3796d1dd2cf96000102208af74b8d39
       4293745c534f13d8b53d2168ce904bc518818c1b507ed9b8fafb570004000000
       07406320a28731a4e1af14d587d2dc6c775434a5e39c1d8df465ec15776cd2bb
       d328c631204cc9d031111cbe583ca3c8ae22f5202768af2654168f169c414e1c
       cd90c52a49200a1dd1f13efa580b819a039d8f1c798856774c526da3a863e63d
       f48f20b5b439
     -
       000000040000000841bb0101201c51ae01ae57eb63da6e5e9277b54613e7765d
       07846e297b374b161d5de3385b20c7fb2d427ebd9d495eaec3d9030734d7394d
       332db68720d2ba65992bde435ac3000120bc0fa16cbda46ebeb4711db71e639b
       299022c6047b5f072d149edb3f4d66bbd00200011800010002000300054a4a00
       070006000400081a1a0009000a04caca1a1a025a5a0c7a7a00010002fe006a6a
       ff000320e77e353fc004ed772ca14d6590b94405aaed55c51c18300d1442c7a9
       64db453007caca04b307349b40401b5e6e904ea1d1dd8699f2fcd16fc75f8424
       d1875c6de22a0335f46d1b8f33dc70ddef2de432a3f22f2bf9c19ebed645889e
       182505646805a2acda1b9c8e49090102206a8250adbd6d7ce0c247fb5d0523b2
       a894c1ef7023e4a64fb48a959c7e62b35c204e0c9a6e742bca7594be91891918
       5b14a5e48e5f48ad022864a032a7b0b3955a000102201a772accc4c9e3476c01
       1c4ddcd677db08ff204d84004d92929cdfc302bafd202013054befab1af498ae
       a5d715c612bb3eb22540f467e85c6c487d9a892e2b069304000000070102208a
       f74b8d394293745c534f13d8b53d2168ce904bc518818c1b507ed9b8fafb5700
       0400000007406320c9aeefb310a510d1d8a7cbea86eaca04de9ca98d9eaefc55
       ce61b745adf460de2076c910669733d1159b71ad9f4057a11a62a17488c8aa80
       b8f1d5360814c9ee922092210b4888a635a2066101c49c4d5a98f81c93e4ba56
       9e3277d1864f03df375a
     -
       000000070000000 8416b0101204ae0ebd152293795ba510cc8f17a497d3f9e02
       e333d913bab8c533a3a52ade6b20c360a0b90ac403e77a707a8fe702f94fcc24
       2c0f5a90586f4bec40ccd959fb1b0001209c02d599900d6410d0b7f61cab1c9c
       f1c166aaf297bea067605831e6fef776350200011a5a5a9a9a00010002000300
       0500070006eaea0004000800090 00a044a4a1a1a021a1a0c00013a3a0002fe00
       ff00baba0100000000000000000ffffffffffffffff0a4a4a07cc451efd508686
```

```
      4040924ec55144045938e926d4fecf4742ca72c784b9cf75e772662c1cfbcce9
      320d0f52180b7e174a77e53af6e04d93fead03207b76f4f43217719d1bec938c
      ae00000102201a772accc4c9e3476c011c4ddcd677db08ff204d84004d92929c
      dfc302bafd202013054befab1af498aea5d715c612bb3eb22540f467e85c6c48
      7d9a892e2b06930400000070102208af74b8d394293745c534f13d8b53d2168
      ce904bc518818c1b507ed9b8fafb57000400000007406320722 9f93f9e8f9c3a
      0c9cc848acdde9d6367551b375a8b07f530a7284b077777e20a2e0081f89426d
      a39e9476d6e63d9f5766f2850a8ad23f01e141388264801b462092210b4888a6
      35a2066101c49c4d5a98f81c93e4ba569e3277d1864f03df375a

   cipher_suite: 0x0001
   tree_hash: a28ecebf4b711cd3e7c001ffdb59018d25cc3db73df2cf96fa9cec51f06145c2
   proofs:
     -
       0000000000000000841b8010120ec18c013e1bd5655e7ae3ef88336ea86f4745c
       ed481497c38d2cae619f11452d20ff535b29e397e38034f59b80c109316ce0cb
       7eb2fd81741f5c81ebb042992cb100012082d746ad98533847d8cb00813fe4bd
       0d44db3b19d7591d5cfb633e4ab040408a020001160001000200030005000700
       06000400081a1a0009000a040a0adada025a5a0a00010002fe00ff00dada0320
       9b5774602220e9dbb098f8fdb9dadb6e3ce88fe3285f50f2b156e87e03bc803f
       0c0a0a09ace396a0150c55e68840400052ced555e139cdef9e0ec0d3886da0f8
       84944fe3368d12bb8ea4d4352ca5e7adbbfee946f7752a6ef933ac1ff1eb526d
       0d6dc3d10cabce21bad451ac66270501022002007a8b243866e24e05f2aa68c8
       013b1d021f9543a983add91490c706dbf137205a3360599b04f22790ec4a7ed4
       9839d9e381e4bac9fc78be0043d6a53de0829400010220c5c774619931531acc
       da3f7d1927ce8be3348edd8bf9659780a139548d4d716420fb8b58629d6c3caf
       075888ce01a0d53b082c4edcd4a6046b6c93997e9f908140000102208c2e1039
       0840e3db8d8e2a0f44c0efab2854b2a7013894c6cedac5fe1437705100040000
       00054063200b69fe27f22cc081efc466503ae8924bea87d8b789da64962dc610
       e89e56528c203e9425d0c47b9ee2abff25a873d526cfd58be76d2c1311812dd6
       69ff4c2631cb20cb1691d9b0099929bece296b85e38e0ccacf60745204907b6a
       3abd16b01d4f01
     -
       0000000300000000841670101205e2a87d497d3f6e2039a7621d8952549554a65
       f54951e3f48223b7e006c1ce4620540314d995b38e40eb05669f8429082de304
       c785eaf23de6b408212f14cf05f20001205dd5f1f48300989389a6420c264c64
       078636bee326769579dd178cc734befc470200011800017a7a00020003000500
       070006000400086a6a0009000a043a3aeaea023a3a0c000100027a7afe00ff00
       3a3a0100000000000000000ffffffffffffffff0c3a3a09fd12d1866a1b5837e9
       40404404dfa8ac135b5c0773986b7cab8cfb298ea48018cf48081313560a3b66
       55a7a133f13510255df5b157890ecf9b1744bfa21a4068a3de4a34c40dafb956
       5b0500010220c5c774619931531accda3f7d1927ce8be3348edd8bf9659780a1
       39548d4d716420fb8b58629d6c3caf075888ce01a0d53b082c4edcd4a6046b6c
       93997e9f908140000102208c2e10390840e3db8d8e2a0f44c0efab2854b2a701
       3894c6cedac5fe14377051000400000005406320 36d41903997f41613f6a82fa
       1729d48719562cc6dfee12ae0bd4514eeab8f71e20e959ba790c00636f43e05a
       fe5f6ab781636c8aef43652ae5db3998e32d79fabb20cb1691d9b0099929bece
       296b85e38e0ccacf60745204907b6a3abd16b01d4f01
```

-
00000006000000008416d0101200cece591dddeb44bdbbf057d8e5c25ef166a0d
00c95341a0ad50f7d1ef69dc4520bdd3452ceb42371ec29240c62c922a29c886
9a25deba467168951a6dd61fc778000120317a01365003e0554c605c6cb7bbe0
b008e9caf78f6f45619750cfeb995e9e5702000116000100020003000500070 0
0600042a2a00080009000a047a7a2a2a021a1a0a0001baba0002fe00ff000100
00000000000000ffffffffffffffff127a7a0f64a35efb7f73d8e88c48d3be4e
e92440403b3da8eb0a95e1daaea6e013ca438cf2c4615aef9c6cfb00dac67c0c
b09628daea3409c4d2d2d0ae982cb75f5ba5fcebc29acf7a04e8b019c45551fa
6acfe20800010220200e4863b5d27138c557267e2adf905b9ff485a7fcf538fa
6bb07ef957e9c26720963167a796c7489ed32f3061464992d1a275025d76b786
72e265f2db6e1c4e55040000000050102208c2e10390840e3db8d8e2a0f44c0ef
ab2854b2a7013894c6cedac5fe14377051000400000005406320 7fa35246a9a5
4288f26e442772cfa64c9f7ebab42ebeb24b4dd762f39aa5092e209fdca5a218
66af8752886ddc20598c404fda9e146bc9794950957d09050966f320b8ac89f1
8646673729d4385f91097c40c1905187033b5fb08a272ad2247bb23b

A.2. Partial Client UpdatePath Handling

These vectors exercise the computation of a commit secret from an UpdatePath without a full ratchet tree. For each case, we provide:

* cipher_suite: The MLS ciphersuite.

* update_path: The encoded UpdatePath.

* tree_hash_after: The root tree hash after the commit is applied.

* resolution_index: The index of the ciphertext to select from the encrypted_path_secret vector.

* sender_membership_proof_after: A membership proof for the sender in the post-commit tree.

* receiver_membership_proof_after: A membership proof for the receiver in the post-commit tree.

* receiver_path_state: The receiver’s retained direct-path private state.

* commit_secret: The expected commit secret.

cipher_suite: 0x0001
update_path:
203cce1a604767a200d6dedebe27fb9f1b417009f32d49274505b99dde6799d3
5720874b4b2fc0e05fdd0b5d92539378c364e2a65b80ae7db896533569c4894a
b6960001209c220b987cfa65764ddf19207c68846361240443de156ceb564168
edd14b1b700200011c0001000200036a6a00050007eaea00060004000800092a

```
    2a000a9a9a04eaea7a7a02dada0c00010002fe00ff002a2a1a1a0320f0c56702
    abdecb522d7d08af5af48e27b30b52cd49f5917e1ce8a6b11b8452de057a7a02
    a14140403047b78d55048fd00fb91dc53cf507b7aa9e4d35666bc622cd0c4f5c
    8cd3c9cbab8989485d05345054d7084b98533f2ce5142f6101ebab6fcdb41253
    8f40780b415f204a8b6445b28e92dc81a7011df86666085c81ea477a02b2d2e2
    ea074fb96076274052209571abd323114ae9dcbfdf609846e888771066aacd46
    63a415885310deca323230b15406063f449d3d9581a0ca2da0b22769226b4035
    067c7bd66e33bb9386b554a026df3e88279cf0f48caee3623d902720253cd2d3
    c8d529f86d72d3230f3736592479fda020b82b8d4ad864e591beba37405220aa
    1704d412cb189471161d70d568c2bb08dba867956d2819329ee0ec322b953d30
    76ab297263b469e305da83b87b56a26c05c04b6b23374d77408fa3c2097ba5b8
    4596f5c5e31546e9e96ed5bec9cf550b20054e60b4a7baa9205e1a987d607910
    cd243c090e20a465584e0558e6998e45334052205f541bc708fc0cbe370b5189
    7d58a1e3b2876608eb980018d1d75d99cc01f970300a57963bd986b34e98af38
    8b3a4931ef18a0ef31cafc240b6881b893f66bae9b6ce7ff5c2769b72be2d274
    a213995f22
  tree_hash_after:
    c646a1ff46f0d34fa8f5a3d1a9784b2d004a2899badd75e29e46f0915110db60
  resolution_index: 0x00000000
  sender_membership_proof_after:
    00000000000000841b50101203cce1a604767a200d6dedebe27fb9f1b417009
    f32d49274505b99dde6799d35720874b4b2fc0e05fdd0b5d92539378c364e2a6
    5b80ae7db896533569c4894ab6960001209c220b987cfa65764ddf19207c6884
    6361240443de156ceb564168edd14b1b700200011c0001000200036a6a000500
    07eaea000600040008000092a2a000a9a9a04eaea7a7a02dada0c00010002fe00
    ff002a2a1a1a0320f0c56702abdecb522d7d08af5af48e27b30b52cd49f5917e
    1ce8a6b11b8452de057a7a02a14140403047b78d55048fd00fb91dc53cf507b7
    aa9e4d35666bc622cd0c4f5c8cd3c9cbab8989485d05345054d7084b98533f2c
    e5142f6101ebab6fcdb412538f40780b0102204a8b6445b28e92dc81a7011df8
    6666085c81ea477a02b2d2e2ea074fb960762720468e751b59a57a38d39e126c
    3832b488f4702183bf22b4a471365a0bb91b9d2600010220253cd2d3c8d529f8
    6d72d3230f3736592479fda020b82b8d4ad864e591beba372032a15c6d69e0d2
    86975b64e298c7edcc971b94107ddf0ea6e04c58d2e22a192500010220054e60
    b4a7baa9205e1a987d607910cd243c090e20a465584e0558e6998e4533000040
    63203e61092b3d7dab8d58aa3a1b9637f442a2743fc838f3c5112f2cb37e5c4e
    baa22061e4a1282956a0b3ea624cc55a739a56b97c56b5c66d02a3785a0a2646
    7a24f4203e07af2a8adbdae583b50ec7dae6b127ba6161b6b80b0caac7aa2bd0
    c7fff755
  receiver_membership_proof_after:
    00000001000000841b5010120a82bc7ea59fdff886b9dc7bb41fed8bc85e522
    1fe8fc35459018345d9aa828432087976588c88d46cb67196a5265d60a2ce636
    94aac1ac932f500ecdf82767137c000120a1525dd8a3ca0e8557bfe073b40cc1
    7e1ad073b0c6b273d6f190e50bdda92a0d0200011600016a6a00020003000500
    0700060004000800090000a027a7a025a5a0a00018a8a0002fe00ff0003206857
    4afb182efa08ece56c785bcbe5e6e444b8a348322f097d94daff4eb140ed0f7a
    7a0c390eebf54ec1bca0e6996377404005110ba84254fa026b5981b445535f33
    46e11776ef9bc31e2b97d55c54b6b6364fadf17fce823b2b38505e41e600552d
    82bf29fbe04a20c9045848c90f23150d0102204a8b6445b28e92dc81a7011df8
```

```
      6666085c81ea477a02b2d2e2ea074fb960762720468e751b59a57a38d39e126c
      3832b488f4702183bf22b4a471365a0bb91b9d2600010220253cd2d3c8d529f8
      6d72d3230f3736592479fda020b82b8d4ad864e591beba372032a15c6d69e0d2
      86975b64e298c7edcc971b94107ddf0ea6e04c58d2e22a192500010220054e60
      b4a7baa9205e1a987d607910cd243c090e20a465584e0558e6998e4533000040
      6320adcdfea6f90a9bcad6fcbec5156ee456487a5c676178e2c2d692786d8e6c
      51202061e4a1282956a0b3ea624cc55a739a56b97c56b5c66d02a3785a0a2646
      7a24f4203e07af2a8adbdae583b50ec7dae6b127ba6161b6b80b0caac7aa2bd0
      c7fff755
    receiver_path_state:
      -
        encryption_priv:
          14a99d34d980f73c68cb1000d9dc018c93fc1754dde02943d1a346066c9fd32b
        node: 0x00000002
        path_secret:
          ed2d3a9bef3d441d5e3a1ee8dcabfe7a4bada7022e2f4c9c301850762f16c535
      -
        encryption_priv:
          80a77d2336ca29c05f56999fd038f5aff875955d01fd6e65358247cdb8e540e5
        node: 0x00000001
        path_secret:
          9775032a7386ce930858f5cb729acf4a8c3f3fb0e5ccceb139f72bfed3349b5b
      -
        encryption_priv:
          812cdd00ad396ae16fac769adc7ef7c83971832d0e7853c7e6f1b4a47b76480b
        node: 0x00000003
        path_secret:
          8697c1b453f41dcb75f849c3469b500b103e439a4b0eefe4e1112042dc0e1890
      -
        encryption_priv:
          c2f97b1ff7b5b2c1b7d62223290e94da5920510e239f7110c25db53dae1368fe
        node: 0x00000007
        path_secret:
          b0518503fc64d7df08fc24261a77b2090362db2c1a7061430ded178d8de110f2
    commit_secret: 166ea7efbd8ea235f3201af7cdc46526bf2937e227a70b76540fa94bd91890ba

    cipher_suite: 0x0001
    update_path:
      203cce1a604767a200d6dedebe27fb9f1b417009f32d49274505b99dde6799d3
      5720874b4b2fc0e05fdd0b5d92539378c364e2a65b80ae7db896533569c4894a
      b6960001209c220b987cfa65764ddf19207c68846361240443de156ceb564168
      edd14b1b70020001180001dada000200030005000700060004000800 09caca00
      0a041a1a9a9a024a4a0a00010002fe003a3aff000320027e7afec2ed2e099fd4
      a798d3a9138da75f8e1bed24be6d166c65a59b06452e109a9a0d174dc6d36741
      a119dcb5bd7b514040832c7b41c31f1f7c692b621bf8b9ac6d572cda9c143b5f
      0a254506cda19c915af7d91dd282496f3084627e26be120a566f650f474362b0
      5807d3317f0a42c60b415f204a8b6445b28e92dc81a7011df86666085c81ea47
      7a02b2d2e2ea074fb96076274052208b18e59a0256d95959d6bfc5c7bc2b0558
```

```
      ff7db101c8c732dba289a9f686890c30c172de81dd344a98df40701cb70dcd59
      e7c607129baef17a9943ab56792b35edcb0e4c6af96a4644b11f4bf0d6a54aa0
      20253cd2d3c8d529f86d72d3230f3736592479fda020b82b8d4ad864e591beba
      37405220632e363edf79a1614213e52de48d2ff59483d9b539a3285e7c555dff
      c023441b3021e456615a2cc89b55056567c8864fb32da2413846f52d735a6091
      5c29bc0a895fb06989b1a6e6181d3c24d88d0f008320054e60b4a7baa9205e1a
      987d607910cd243c090e20a465584e0558e6998e4533405220c210830bf7d8ce
      9716e4bfe3e99cf9bee3d9c7e61ca1ded259969e18e667bf73305dc0ad3104f7
      22965fab1bcfcf99efa0907fff4f04b01a60af892ebda156fde220e7bb3a489c
      f030176c175b18f84ef7
    tree_hash_after:
      f3ff4ad42554596c35b62d3daa9a1832b0d5d2fbe291514aa2b882211b9c67d5
    resolution_index: 0x00000000
    sender_membership_proof_after:
      000000000000000841ba0101203cce1a604767a200d6dedebe27fb9f1b417009
      f32d49274505b99dde6799d35720874b4b2fc0e05fdd0b5d92539378c364e2a6
      5b80ae7db896533569c4894ab6960001209c220b987cfa65764ddf19207c6884
      6361240443de156ceb564168edd14b1b70020001180001dada00020003000500
      0700060004000800 09caca000a041a1a9a9a024a4a0a00010002fe003a3aff00
      0320027e7afec2ed2e099fd4a798d3a9138da75f8e1bed24be6d166c65a59b06
      452e109a9a0d174dc6d36741a119dcb5bd7b514040832c7b41c31f1f7c692b62
      1bf8b9ac6d572cda9c143b5f0a254506cda19c915af7d91dd282496f3084627e
      26be120a566f650f474362b05807d3317f0a42c60b0102204a8b6445b28e92dc
      81a7011df86666085c81ea477a02b2d2e2ea074fb960762720f1523fc5c6a1c7
      45b088e8008ec89031b8578401de51025cc1d1e6703f0a567900010220253cd2
      d3c8d529f86d72d3230f3736592479fda020b82b8d4ad864e591beba3720eb3a
      5c40422d97949ebaf5f57440c71fe27a12aec1a64edf72ac593b9c158f770001
      0220054e60b4a7baa9205e1a987d607910cd243c090e20a465584e0558e6998e
      45330000406320a306a778d4e4ce00e58980fead0ed7e4ad89911e817d417f55
      86f93be623aa692043952f6ac664f0aa3b16bb429fa6aa8b302c9fab869f8c20
      6a6f5d0947b23fa4208e2264b11acb9cfdc56dbfcdc44c6ae6167f9b2e184499
      198d62d7f8b9f3c450
    receiver_membership_proof_after:
      000000070000000841a4010120be7690a2e3bd726d3bf66742bd5815295c7732
      71d45cc3fb17bda3f610c3b93e204798d989c330b1291f46926f649bc8918352
      bfe41ac73941fb76e726d27d38db0001202cfb5a7ee155995bc0fce26b3727b1
      27ebd3e5b10272c922b1f95e68d944414a0200011800019a9a0002caca000300
      0500070006000400080009000a04aaaa3a3a028a8a0a00010002fe00ff00baba
      0100000000000000000ffffffffffffffff0baaaa08ced72c5c65290918404003
      bb313b25f62a2509805aea793bbe01f53010c3676724d605425b3016cf0a1441
      c35b2e50360920747ec1c1c920871fe58e2a3246ec07f316414088bfe0620901
      0220a461c48056943854d24a4b27a57afcaba53a6aa1a0894dfe034753ac37c4
      0e692074b9295d3c2402d7f7c5b76e3ed4bc848ca8ad4db59889172207d98da8
      f1ce85000102206ea5fd8c8b1335f7eee35cd5d662b96e76853732e60f94763a
      5d2e0c1289be2920d133844620ca1496e102434c204662a6991a1e85fd7b65d4
      72f7a748d8619fa800010220054e60b4a7baa9205e1a987d607910cd243c090e
      20a465584e0558e6998e45330000406320a4cfe8f092da8aff198f18b9e216cc
      8e7e1904fc75807d6a3f7484e12e9edf2220f537c870891457cbc9672437b1b8
```

```
    5d3f04cbc00c91b533f7475961b99a51f97220bcc283ee53996ff61407eeb2ae
    bc230b3d10aa35f678ca6a41fe0e387526edab
  receiver_path_state:
    -
      encryption_priv:
        dcf47362ec49a730ced67943cf549a6f7f9428d1acc185ecb2cdec151047c42e
      node: 0x0000000e
      path_secret: ""
    -
      encryption_priv:
        890782c6a3c60142f26e81bd8c47080b11ca3de16d19c9f62246f563da146660
      node: 0x0000000d
      path_secret:
        157b58a1b7c3274fed9fa8d0d7d7e23b5b31beb105516b5fd68eae80008fd058
    -
      encryption_priv:
        45171cc19457fd20b782ca663457e9c76d77ad4b2abe775cd44e0aeac82aff26
      node: 0x0000000b
      path_secret:
        e1e57659be2e2608cd34638129378bfa46beff61d93aa6e6028d2c69e80fdc72
    -
      encryption_priv:
        c2f97b1ff7b5b2c1b7d62223290e94da5920510e239f7110c25db53dae1368fe
      node: 0x00000007
      path_secret:
        b0518503fc64d7df08fc24261a77b2090362db2c1a7061430ded178d8de110f2
  commit_secret: 166ea7efbd8ea235f3201af7cdc46526bf2937e227a70b76540fa94bd91890ba

  cipher_suite: 0x0001
  update_path:
    203cce1a604767a200d6dedebe27fb9f1b417009f32d49274505b99dde6799d3
    57207d118f039fa24cf95395e8d69d70a294a76532c66c305fe89abc36114242
    eed00001202815ebba746ff92411b00ca7c632886a52a06b865a5632bb87f7cc
    0c291d694b0200011c00010002dada00036a6a00052a2a00070006000400087a
    7a0009000a04baba3a3a02baba0c00010002fe00ff007a7a5a5a03200e348f21
    953c75f2f76e96d4d5aae7d41e5d1298a26da122b97fc514baa820870d3a3a0a
    0b908d3ec43bd7906dcd40402bdbad74fd889074a2a7b7e3ac2acc88a0efc2dd
    5e9ba76d77ed6a7773234b4218449d1c957ba55acadd013004c48a46b5a4f43d
    d1967da019338463aa7afd09415f204a8b6445b28e92dc81a7011df86666085c
    81ea477a02b2d2e2ea074fb96076274052205l6f4e5c691b7b3639eabeabb8fe
    a599c24affe085beaaf2c41d64c0ba40185a3026f5cc887e5c4f6ce9d68254f6
    6e05c578d94d36e7aca0e515ac2f1c30e9a661fc1b271eb7f034e3bb15a9d94a
    eb7fb220253cd2d3c8d529f86d72d3230f3736592479fda020b82b8d4ad864e5
    91beba3740522042c553d770515460bf71ed1a643414592240b7c5956f6e3b6d
    b6c3dd0b38fa3b308c14bfd909ebdf31811a8a3b9dd66948ead4a45df4b9ab58
    05f91af4b4200c337f6332d4a0f8e96538f804e2037415dd20054e60b4a7baa9
    205e1a987d607910cd243c090e20a465584e0558e6998e45334052206b64ffb3
    ce1f000665813e8e53c10b3c285874f250f3ae2fa68ac3b0474586033085408f
```

```
    19f753154197ca77fd4db2349c41f0f84c56599733bd2bf3c450da5e426d1020
    0092f62fc9527c024377d91fe9
  tree_hash_after:
    994700a7ac4d1ecb9e71844456bd60809dc75f592f3ca4afa15084270ae428dc
  resolution_index: 0x00000000
  sender_membership_proof_after:
    000000040000000841bd0101203cce1a604767a200d6dedebe27fb9f1b417009
    f32d49274505b99dde6799d357207d118f039fa24cf95395e8d69d70a294a765
    32c66c305fe89abc36114242eed00001202815ebba746ff92411b00ca7c63288
    6a52a06b865a5632bb87f7cc0c291d694b0200011c00010002dada00036a6a00
    052a2a000700006000400087a7a0009000a04baba3a3a02baba0c00010002fe00
    ff007a7a5a5a03200e348f21953c75f2f76e96d4d5aae7d41e5d1298a26da122
    b97fc514baa820870d3a3a0a0b908d3ec43bd7906dcd40402bdbad74fd889074
    a2a7b7e3ac2acc88a0efc2dd5e9ba76d77ed6a7773234b4218449d1c957ba55a
    cadd013004c48a46b5a4f43dd1967da019338463aa7afd090102204a8b6445b2
    8e92dc81a7011df86666085c81ea477a02b2d2e2ea074fb96076272067516442
    c1258339c35f1addea0a954a9cbc17d436b2aca39956d897e5df386200010220
    253cd2d3c8d529f86d72d3230f3736592479fda020b82b8d4ad864e591beba37
    2055788e99113a3fa9d7479ff9d9e3d5159b7da53d84a9c4f9f5a041b81040d0
    9d00010220054e60b4a7baa9205e1a987d607910cd243c090e20a465584e0558
    e6998e45330000406320dfce501875a0a0aaf2337df8b01802379dcf1caf71f3
    5ba82c6073162670d08d2085d8f7ac31ce581d917a28a2ee09bdf3de05d3b712
    3d49fe979f86dc578b1e7d2049c3a626cee5a832083a4b502f022f43bbea96d8
    a2d6a7f666ebc021cbf3d20e
  receiver_membership_proof_after:
    000000000000008412d010120e4ad1fbca5bb4b520d8347b097ac1deecf95bc
    232608ae5fb360e93b06a87e42200f490bbc5ec4d0db3028e310484ff6d55458
    49842f3d0cf2840d9edb6894f64c00012074f89864f90bf1acb346c5caf48f11
    1149c9b7980cd0717abeb4e5da576a4e570200011c000100026a6a2a2a000300
    0500070006dada000400083a3a0009000a044a4adada026a6a0a00010002fe00
    0a0aff00032083f6b8c1fbb3464b1e71243ceaca960c00454669d1ad34cab37f
    140cadcab114074a4a04466a3e41404018008efbb0fd2fa00a0e3f829c78ad5d
    aac1ba57759bcd02e4d649db25a06d5238466c34228526dae97f91a6552665f1
    ba9dd476d5585665f86ff0223bbd710d0000010220054e60b4a7baa9205e1a98
    7d607910cd243c090e20a465584e0558e6998e45330000406320a90d4563c6a0
    ae0417ab3110f1ba685928334659547742O1b0a69e8c457dc6ad20c0d2b83fa7
    6a6a182e97682d717acc9427d8e7e4dbaee5df157b72fa332732a520fd5f669d
    334ecf938b0d0d23e566dbe6b591143bed5678222f5dffc9e2b76165
  receiver_path_state:
    -
      encryption_priv:
        3d5884f022a9574675878b07f45f8fb242b643a3fc12d6b213e07850cd7e4ce2
      node: 0x00000000
      path_secret:
        6b41b40b704c8352822ad18bf864fdd1b4e7814349e82afe9f6ad3dcd65940c0
    -
      encryption_priv:
        5487842769722ae26437e2fb20cf6a2b4cc888a968ed18c8d76620d3e369ed7c
```

```
      node: 0x00000007
      path_secret:
        e99894734dcd0b4492b28fb3a1acc803fe305c5a6c040877da7adfe1bfd1a01a
  commit_secret: 166ea7efbd8ea235f3201af7cdc46526bf2937e227a70b76540fa94bd91890ba

  cipher_suite: 0x0001
  update_path:
    203cce1a604767a200d6dedebe27fb9f1b417009f32d49274505b99dde6799d3
    5720171ea1a5a623810898c2b3bde08b015184637afdd1151094a20ac4b71df9
    6f6e0001208f2ddc42d16b933c60dbc3c4997b9767dd04bb8efa79c6451c96f1
    e4704658b50200011a4a4a0001000200030005000 7caca0006000400086a6a00
    09000a04dada9a9a022a2a0a4a4a00010002fe00ff0003206640670d4a847297
    1decc12c8a0a2c39ee0db7c9ce8dadafcd513873ce3a869611dada0e8fb9b19d
    93bd4777cff634b3e7f940405ca54184b8965ed8772b67e6d952f4a9f09cd3ea
    a3c533f2f1c730869e4afe488fdf5d79f4aba1dc622ef181c5677f25219a16c2
    cf60ee4528d7a80eaacc61064203204a8b6445b28e92dc81a7011df86666085c
    81ea477a02b2d2e2ea074fb9607627405220195c4cb1751c8d48ed8008655fe0
    e616254f289134d20de13c375ed02ac24f3b304bd8a6d0cb8e4df48bd58dcdee
    bc5f091f3cbe4ac61e1fe9fd3a1a3b25e4dcee869a4a344924bc6c1b2fa924a6
    95deb720253cd2d3c8d529f86d72d3230f3736592479fda020b82b8d4ad864e5
    91beba3740a4204e240606317e5316f127ab0421a0b082787328a37cbaa5f031
    3381a886f2d02a3085c276889b160f9979942d061dc81ea2910c12165c77a177
    c29593099f76dc74b9e7374f83bce1bd70b6f53d17d3ac502037f18126ba1841
    8335cfc97dafef35ae3fe3c8db164ac86d74d44d51227e772530bb7660536fd6
    bd5420332fa29907d4ed982f01dd7b1ff82523ab2ca75356d87af423eef34e60
    f826274541b72d30665220054e60b4a7baa9205e1a987d607910cd243c090e20
    a465584e0558e6998e453340a420d76f54753442b529974a59c8961f9531d260
    9ba3c47e3b832c2c26a1c2046e13300423b4cba28de967264261c41baee72ab0
    906439f3d97ebfbc241c4106e8a49649f827b97f619f7e07d017d1be76c6b920
    406c868040b089692ce237a5e37a94ebdb9c2494c670d63f0214e1bfd646c540
    3011c3f702cfd6f3e3150bfcda0622d02c63ba56ef8c01a05c69e3b8726125b2
    966a0ed7f6faf78886236eaf46feebe5a9
  tree_hash_after:
    5a5288f0acb72603f72ab437744543de23debdb57fd571a567e7432efb9a1bff
  resolution_index: 0x00000000
  sender_membership_proof_after:
    0000000000000000841bd0101203cce1a604767a200d6dedebe27fb9f1b417009
    f32d49274505b99dde6799d35720171ea1a5a623810898c2b3bde08b01518463
    7afdd1151094a20ac4b71df96f6e0001208f2ddc42d16b933c60dbc3c4997b97
    67dd04bb8efa79c6451c96f1e4704658b50200011a4a4a000100020003000500
    07caca0006000400086a6a0009000a04dada9a9a022a2a0a4a4a00010002fe00
    ff0003206640670d4a8472971decc12c8a0a2c39ee0db7c9ce8dadafcd513873
    ce3a869611dada0e8fb9b19d93bd4777cff634b3e7f940405ca54184b8965ed8
    772b67e6d952f4a9f09cd3eaa3c533f2f1c730869e4afe488fdf5d79f4aba1dc
    622ef181c5677f25219a16c2cf60ee4528d7a80eaacc61060102204a8b6445b2
    8e92dc81a7011df86666085c81ea477a02b2d2e2ea074fb960762720ba5c8746
    5b31566e3ab2f9b2b7de27aec182c62f1c722d0b12a572ae1455e8fd00010220
    253cd2d3c8d529f86d72d3230f3736592479fda020b82b8d4ad864e591beba37
```

```
    20d7770bdc319b16fc59af6d8149a91b124e75921db7b86f6308129a05eb3245
    d400010220054e60b4a7baa9205e1a987d607910cd243c090e20a465584e0558
    e6998e45330000406320362dc9b7d6b776bd49f2202b48f1552dda616a39732b
    e2cce6f1196d7c8a41a620981d5a8c1b10f759f94c6c068f51ce5863f12d29b6
    cd2d2533ef5966b2a93b312068deff53ba52391f08c31b82b86080722a139927
    4a5acb3ea0fa510ca83a8a8d
  receiver_membership_proof_after:
    0000000400000008417501012 09c10cc0ec3fc1658e890bd498579a875098211
    8dee84969e3fece89d859fd32a20ee30c3b3ff1d10fb7a5d551ec22a604dbe26
    83d9ea959747480f0e668817fffc000120feff7eb14dcfa1ca5d199d2ff31a2a
    27465374dd7e4d01286d67d240cb8c409a0200011caaaa000100020003000500
    076a6a0006000400080009000ababa2a2a041a1acaca028a8a0a00010002fe00
    0a0aff000320e38c41e1c68f7ed69df493a8562d80dfc3823463b745b9384bea
    7187ff9e514807caca046b8df4d24040c141cd422d250479c46a5b054728aee7
    1f0182c52ad0136149aa1adeed52abe26b3637f2dbecec1dc7221e66aa1a3ecc
    d268e4b106949605edfd2218234d4c08000102209357ef216ef60d18dd74bb44
    23b47a10ef01bad713756c54011ec4818f06e02b206208dd378c8e494897ee9d
    18d21498531a0c8df1933ca874097307747de17fb00400000005010220054e60
    b4a7baa9205e1a987d607910cd243c090e20a465584e0558e6998e4533000040
    63200fa803fbedc3650cfb18b6bd87e66fc9e0004e703fcf714e70608eb28f14
    a8c7205d529bb5877721e98aa3cc576d48ebe93e940bb2ea89a1451eec1fad5e
    5b849c203aff10bb92294e2569c63ec24b9dc8212e2d8755a219e7c95ceacc7a
    fdec1cb2
  receiver_path_state:
    -
      encryption_priv:
        cb39867f27c096e2122a161bf0ec66460d79b0ef45eb4fa0bd4b59385c6f6da2
      node: 0x00000008
      path_secret:
        dae594efa82228d6b0620d7fffae552987a9f1df51d6eda005e0056191ebfb28
    -
      encryption_priv:
        2f42e1db6153f72ceb53863591c1b4b038e1528cd9869f671fa6c8b01afbc994
      node: 0x0000000b
      path_secret:
        133b40377b8d1fc72c5079756a23d82fce024965405ce0ae3288cade9626f783
    -
      encryption_priv:
        0585944781374f947450f721741f58c3aaf81c613d92336e58227da18829a441
      node: 0x00000007
      path_secret:
        1f84214141acb58e53f6ad994a00a51f25c25d9cc9035eb57c7bc12087cbd531
  commit_secret: 166ea7efbd8ea235f3201af7cdc46526bf2937e227a70b76540fa94bd91890ba
```

A.3. Partial Message Syntax

These vectors exercise the TLS presentation syntax for the new Partial MLS structures. For each case, we provide encoded instances of:

* CopathHash
* MembershipProof
* SenderAuthenticatedMessage<Welcome>
* SenderAuthenticatedMessage<GroupInfo>
* SenderAuthenticatedMessage<PublicMessage>
* SenderAuthenticatedMessage<PrivateMessage>
* AnnotatedWelcome
* AnnotatedCommit

```
cipher_suite: 0x0001
copath_hash:
  209f1c43dd0988a69de12ae2d9d95846167685d501f23a3be2f25e0c28dc28c5
  eb

cipher_suite: 0x0001
membership_proof:
  0000000000000000440f201012064a2512b39ad7bdb8c7d0afe208cf617efeecc
  f0c3555ffc04b9198c71283f572069b9a1f249a540917dc99eee145c76d5751b
  68c141b192d5866f15cbad0cd70d00012085e096402f7b4d9dac66567adbbf02
  bd138989d40ade7b7446b410fe03ab32a4020001160001000200030005000700
  060004aaaa00080009000a04baba4a4a02baba0c00010002eaeafe00ff007a7a
  0100000000000000000ffffffffffffffff06baba03eda60a4040f15c7c4801e7
  31a7ac0ac2237107931962914286 32de89458dbc20d38d4a6bacfaab948e041d
  951d44115bd889de7560032f9f00874f96ad4e67455cece3a10200004042209f
  1c43dd0988a69de12ae2d9d95846167685d501f23a3be2f25e0c28dc28c5eb20
  31bbfcf6f3ebcc33735c9049c7107ea29b709039b545c875865a63da5a937365
```

```
   cipher_suite: 0x0001
   sender_authenticated_welcome:
     000140762058e5cd3e18f52bab22383d1689fce2adb02f7fcf0e477e53b118a7
     0ccc4a7ffa20704d804b3e81578d2b1f7d8c0168627d2e94e34ee5e5bdfa5425
     68e24196913b33a109f00b65a33fa89da774ead38ae94cc494afc70ad86e10dc
     df314504b3f2b654d6633645455464eb4556a31866713797fa4440fad0cb9901
     47ae620fae037c5429080d1503cec3e81a98beaf883d177c616dd55cfd8a8e4b
     16008dec94538f02c120e657570bb2816e97366038f525f6a5e9921353715bb5
     82272f06d2c64429e523032992e4f2a8d8d27679482dde5c50a24f85ed57558b
     f1b738de92df788370215585a1380ed8c8f95dfed734ff021190547f2d51ecf7
     b3ef4ec9c3c0537b60db47c893fb661c5b1c23d8d37fc94d7e55e26bbe4508a7
     a31508620ec41b97715eda35ad3205c811b747419feeb65e5d644139613307f8
     8ed3a0f899bdc7118926764f04d9530f5d639711272067c6b4bf39c51cf1149a
     2a05e2c54bd46cd584d75951b72f03457d5e72aa7513000000000000000440f2
     01012064a2512b39ad7bdb8c7d0afe208cf617efeeccf0c3555ffc04b9198c71
     283f572069b9a1f249a540917dc99eee145c76d5751b68c141b192d5866f15cb
     ad0cd70d00012085e096402f7b4d9dac66567adbbf02bd138989d40ade7b7446
     b410fe03ab32a4020001160001000200030005000700060004aaaa0008000900
     0a04baba4a4a02baba0c00010002eaeafe00ff007a7a010000000000000000ff
     ffffffffffff06baba03eda60a4040f15c7c4801e731a7ac0ac22371079319
     6291428632de89458dbc20d38d4a6bacfaab948e041d951d44115bd889de7560
     032f9f00874f96ad4e67455cece3a10200004042209f1c43dd0988a69de12ae2
     d9d95846167685d501f23a3be2f25e0c28dc28c5eb2031bbfcf6f3ebcc33735c
     9049c7107ea29b709039b545c875865a63da5a937365

   cipher_suite: 0x0001
   sender_authenticated_group_info:
     00010001207c7e9b2e3b6a9b4549a5ef18959665038ed1f1b24c3c8003d03d24
     08120517010000000000000022063b4f9c3710664d0fc52301e314d4bea7965
     e6f6f56aa4e21e0e4d24087f7f6e208d3570c404a1443e748f9b88c4ab941fd1
     e8b6aaac79f003770e88ad6bcd7eaf0030eaea09fd27f2252a54c9055a000421
     20b90f28610f9ac989424704726c3ddcced46940ccbbd54d9870962ec4b7f43e
     6220f1b477e67b97bbe5d25fa52db5792258b8fa619fdadd487698f1409871c3
     b1a9000000004040ec03cab738999361a558979dbd832d7baff1c154216d2ad8
     810897215e4c5f7ad277274a0cef81ecc02e3d6ead0448cbdb65a9aa54eb8d20
     d9b114aa653f900000000000000000000440f201012064a2512b39ad7bdb8c7d0a
     fe208cf617efeeccf0c3555ffc04b9198c71283f572069b9a1f249a540917dc9
     9eee145c76d5751b68c141b192d5866f15cbad0cd70d00012085e096402f7b4d
     9dac66567adbbf02bd138989d40ade7b7446b410fe03ab32a4020001160001000
     0200030005000700060004aaaa00080009000a04baba4a4a02baba0c00010002
     eaeafe00ff007a7a010000000000000000ffffffffffffffff06baba03eda60a
     4040f15c7c4801e731a7ac0ac223710793196291428632de89458dbc20d38d4a
     6bacfaab948e041d951d44115bd889de7560032f9f00874f96ad4e67455cece3
     a10200004042209f1c43dd0988a69de12ae2d9d95846167685d501f23a3be2f2
     5e0c28dc28c5eb2031bbfcf6f3ebcc33735c9049c7107ea29b709039b545c875
     865a63da5a937365
```

```
   cipher_suite: 0x0001
   sender_authenticated_public_message:
     207c7e9b2e3b6a9b4549a5ef18959665038ed1f1b24c3c8003d03d2408120517
     0100000000000000020100000000000200010001000012048af21491104bbdc4d
     a4f2f622d4df5d6e867af73c4448ddc483d27c5488623f209ea1a3bf83f48f48
     b61ed0ab9254e12b295998b588b6fc4d89eb6efcbedc594620bb7efc012e03ba
     1bbc5a3b8eeb8ae8ebedc0f7d638cb110227d619d95cafcf2900012040693f35
     f79d8affae7fabb5878bd94123ccb1c8a356b2bfdee4d823d0ab686602000116
     0001000200030005000700060004000800091a1a000a046a6a3a3a02dada0cca
     ca00010002fe00babaff000100000000000000000ffffffffffffffff076a6a04
     c7ad4a2b4040c882e57614da1acda9c5b8783b6a2454ec2ade0d02edaf81d581
     2c4022bfe3b6aed49e8f1519b780e6fbab187637f435c1945c6657ace643fd21
     f4a1bf71330405aaaa024c224040be16a33d0aa8c946ecdbef19ef96b7ab4714
     52831cf222f0f8a5614eddcf84311dfd1e76b0680e0693f6e585abcaff96a0c7
     1752b5fb514c05111727f619080e40404997cd96620a5652feed5915682db385
     86b5f8737431f7813baa14aad13d477d62ec059a5d3d9aee5921ff7abcefb66f
     a9c7ff6e1346c0246b00fcfa39ddef062009714aa426ec5a850a7f6c7d057d22
     7a165f6e9f0bed45d694913036401d8ce60000000000000000440f201012064a2
     512b39ad7bdb8c7d0afe208cf617efeeccf0c3555ffc04b9198c71283f572069
     b9a1f249a540917dc99eee145c76d5751b68c141b192d5866f15cbad0cd70d00
     012085e096402f7b4d9dac66567adbbf02bd138989d40ade7b7446b410fe03ab
     32a4020001160001000200030005000700060004aaaa00080009000a04baba4a
     4a02baba0c00010002eaeafe00ff007a7a0100000000000000000fffffffffff
     ffff06baba03eda60a4040f15c7c4801e731a7ac0ac223710793196291428632
     de89458dbc20d38d4a6bacfaab948e041d951d44115bd889de7560032f9f0087
     4f96ad4e67455cece3a10200004042209f1c43dd0988a69de12ae2d9d9584616
     7685d501f23a3be2f25e0c28dc28c5eb2031bbfcf6f3ebcc33735c9049c7107e
     a29b709039b545c875865a63da5a937365

   cipher_suite: 0x0001
   sender_authenticated_private_message:
     207c7e9b2e3b6a9b4549a5ef18959665038ed1f1b24c3c8003d03d2408120517
     0100000000000000201001ce7e4eb2f58bb082f1793af643a4e2853aa282aa8
     3443e3edc9c2121e407393d944d103a5c23e4f86f2513c6096948532817b4878
     fa554e3b57503047caf6c2f23022083286468a7bc86d9c544c7402c02cecef6e
     f32688ac8d13581932bdc2a1f068fbef33a88f45c95ff8614495d98e64081e30
     2e459af3d5d8c4e3e5b56ecb237cadf68710ab6635013086ee3d50d0de000000
     010000000440f9010120032c58f878af02746e47d6a28f9221380a7c2c9d3a4d
     034b987d16fc46a4a87e2003aab15da87002cf647bc963d0448374b29849a35e
     4778ba6bc6c61c9e5c15ae000120d9e342b1794d9dff31be57aa8319937760b5
     ac421590264a20ba4c78d81bf4b80200011600012a2a0002000300050007000 6
     000400080009000a04eaea4a4a028a8a0c00010002fe00eaeaff008a8a010000
     000000000000ffffffffffffffff0deaea0a0ec5a5cf5f7c13525ed64040212a
     8495b44eee0b93e7fe45c5400718864a62b25fe480fbc1bd565e3fdd4398cee9
     42780caf63c74d62d74711d268353e562d66862b90f151896808d14cbb030000
     404220f7c34d339a04a639dc296056c5c36c2160f2cc2bc0803252b60ecd3002
     925dc82031bbfcf6f3ebcc33735c9049c7107ea29b709039b545c875865a63da
     5a937365
```

```
   cipher_suite: 0x0001
   annotated_welcome:
     000140762058e5cd3e18f52bab22383d1689fce2adb02f7fcf0e477e53b118a7
     0ccc4a7ffa20704d804b3e81578d2b1f7d8c0168627d2e94e34ee5e5bdfa5425
     68e24196913b33a109f00b65a33fa89da774ead38ae94cc494afc70ad86e10dc
     df314504b3f2b654d6633645455464eb4556a31866713797fa4440fad0cb9901
     47ae620fae037c5429080d1503cec3e81a98beaf883d177c616dd55cfd8a8e4b
     16008dec94538f02c120e657570bb2816e97366038f525f6a5e9921353715bb5
     82272f06d2c64429e523032992e4f2a8d8d27679482dde5c50a24f85ed57558b
     f1b738de92df788370215585a1380ed8c8f95dfed734ff021190547f2d51ecf7
     b3ef4ec9c3c0537b60db47c893fb661c5b1c23d8d37fc94d7e55e26bbe4508a7
     a31508620ec41b97715eda35ad3205c811b747419feeb65e5d644139613307f8
     8ed3a0f899bdc7118926764f04d9530f5d639711272067c6b4bf39c51cf1149a
     2a05e2c54bd46cd584d75951b72f03457d5e72aa7513000000000000000440f2
     01012064a2512b39ad7bdb8c7d0afe208cf617efeeccf0c3555ffc04b9198c71
     283f572069b9a1f249a540917dc99eee145c76d5751b68c141b192d5866f15cb
     ad0cd70d00012085e096402f7b4d9dac66567adbbf02bd138989d40ade7b7446
     b410fe03ab32a4020001160001000200030005000700060004aaaa0008000900
     0a04baba4a4a02baba0c00010002eaeafe00ff007a7a010000000000000000ff
     ffffffffffffff06baba03eda60a4040f15c7c4801e731a7ac0ac22371079319
     6291428632de89458dbc20d38d4a6bacfaab948e041d951d44115bd889de7560
     032f9f00874f96ad4e67455cece3a10200004042209f1c43dd0988a69de12ae2
     d9d95846167685d501f23a3be2f25e0c28dc28c5eb2031bbfcf6f3ebcc33735c
     9049c7107ea29b709039b545c875865a63da5a9373650000000020000000440f5
     010120bb084105e658fdc5c68f6582d8530a8f85f3afa4f2cd74deeaa83cfb1f
     13a82920a49d7a47ae396ecd25aff26a0564fc612b2a4833dce23d21d3b2349c
     2df753900001201d220eacd2dfb7f74f5433cbe03c65d88505c00897756936b2
     f17ca0b111b4e10200011a00018a8aaaaacaca000200030005000700060004000
     080009000a04dada8a8a02dada0aaaaa00010002fe00ff000100000000000000
     00ffffffffffffffff07dada04b8691d0b4040ab38a42005e0d82eb36f64bb23
     53719ddb63fe2b81a845efd470c56f7e33ca92690379e0e7b4705b575a4b4760
     bce850c237deac402d6781029df93835deb7090000404220caf009ad02a57a48
     feb8d64d055509e9a81edba8d325e442cfe75e006a520006208d7c8373e1f22a
     aa107b62358cd2f11e58568afc187ac1b6e58b10d651a96cc1

   cipher_suite: 0x0001
   annotated_commit:
     00010001207c7e9b2e3b6a9b4549a5ef18959665038ed1f1b24c3c8003d03d24
     0812051701000000000000000201000000000003000120807 88addc360000254
     1a0690b8f0b37d50240bc55d01b91919ad74f8a62af1542069b9a1f249a54091
     7dc99eee145c76d5751b68c141b192d5866f15cbad0cd70d00012085e096402f
     7b4d9dac66567adbbf02bd138989d40ade7b7446b410fe03ab32a40200011600
     0100020003000500070006000 4aaaa00080009000a04baba4a4a02baba0c0001
     0002eaeafe00ff007a7a0320acf2364c319d5c0065cee01e0fcbcd73a1da0639
     f3075e5c6ac153009efd434c06baba03eda60a40402b25298dcbdc1f0c8079d4
     5351aec48c0aa459b9c7b49bf20bc7ec63acc143d508cef375af699f6ff6fcf3
     1f63779dfa4e166eed1cae44ca67c0ce05964fec0240ea203008b68d4dde6fff
     5038b36d7548c1a68ccba2b77cc3cf93cac80177d5d56a374052208981dc1253
```

```
57209b2997a61fbf44b78b14df4e2d4fd718ecdd17b8feeae71379304c058fef
deb05c95dc59c754eddddf37dd33ad6fc7acd60660dcc42fbc619c728d578eb
f7603656de13541fbf4969fe2001d032164a7bde45ff05ffb49ae9bbbb79c2ee
54dc6f7946257a9a5a4cf246364052207c19b20d43d26bd17ff1c2b716d0204a
75522630fa31b0bb76fb15506b07b15930cc55590c380a0d6fb56e92d826ebca
4815848ebf688b5dfa02f0313e2a5699c3484ac2b98e3cd731d4aba986570d16
334040285f52376ecd46ff1ce3303b05e940367a2819b92d41a0e1b47a93a9db
78f119e3dea5d61cc0387841c47b221c76b2d1d658e2c53fd73c8d02abe77aa7
44e20d209e7994867f101cc05678b5b58de43991017010cf7a57fc50cbbe6488
e8144f1d20b075631457bb8edd1341cd4a81e5daa4ca8c32ce63c41c9c788286
21c1405410010000000000000000440f201012064a2512b39ad7bdb8c7d0afe20
8cf617efeeccf0c3555ffc04b9198c71283f572069b9a1f249a540917dc99eee
145c76d5751b68c141b192d5866f15cbad0cd70d00012085e096402f7b4d9dac
66567adbbf02bd138989d40ade7b7446b410fe03ab32a4020001160001000200
030005000700060004aaaa00080009000a04baba4a4a02baba0c00010002eaea
fe00ff007a7a01000000000000000ffffffffffffffff06baba03eda60a4040
f15c7c4801e731a7ac0ac22371079319629142863 2de89458dbc20d38d4a6bac
faab948e041d951d44115bd889de7560032f9f00874f96ad4e67455cece3a102
00004042209f1c43dd0988a69de12ae2d9d95846167685d501f23a3be2f25e0c
28dc28c5eb2031bbfcf6f3ebcc33735c9049c7107ea29b709039b545c875865a
63da5a93736520669ab6fd05f86e4932cfe025627e37c35a5406d59dd6b6edb2
7dd33c438b53b401000000000000000000000004416b01012080788addc36000
02541a0690b8f0b37d50240bc55d01b91919ad74f8a62af1542069b9a1f249a5
40917dc99eee145c76d5751b68c141b192d5866f15cbad0cd70d00012085e096
402f7b4d9dac66567adbbf02bd138989d40ade7b7446b410fe03ab32a4020001
160001000200030005000700060004aaaa00080009000a04baba4a4a02baba0c
00010002eaeafe00ff007a7a0320acf2364c319d5c0065cee01e0fcbcd73a1da
0639f3075e5c6ac153009efd434c06baba03eda60a40402b25298dcbdc1f0c80
79d45351aec48c0aa459b9c7b49bf20bc7ec63acc143d508cef375af699f6ff6
fcf31f63779dfa4e166eed1cae44ca67c0ce05964fec020102203008b68d4dde
6fff5038b36d7548c1a68ccba2b77cc3cf93cac80177d5d56a3720cf7195ab3c
09022169186bf7e44aa26eabcf1f422dcb384f2f14828807862e2b0001022001
d032164a7bde45ff05ffb49ae9bbbb79c2ee54dc6f7946257a9a5a4cf2463600
004042209f1c43dd0988a69de12ae2d9d95846167685d501f23a3be2f25e0c28
dc28c5eb2031bbfcf6f3ebcc33735c9049c7107ea29b709039b545c875865a63
da5a9373650000000200000004411901012 0bb084105e658fdc5c68f6582d853
0a8f85f3afa4f2cd74deeaa83cfb1f13a82920a49d7a47ae396ecd25aff26a05
64fc612b2a4833dce23d21d3b2349c2df753900001201d220eacd2dfb7f74f54
33cbe03c65d88505c00897756936b2f17ca0b111b4e10200011a00018a8aaaaa
caca000200030005000700060004000800090 00a04dada8a8a02dada0aaaaa00
010002fe00ff000100000000000000000ffffffffffffffff07dada04b8691d0b
4040ab38a42005e0d82eb36f64bb2353719ddb63fe2b81a845efd470c56f7e33
ca92690379e0e7b4705b575a4b4760bce850c237deac402d6781029df93835de
b7090001022001d032164a7bde45ff05ffb49ae9bbbb79c2ee54dc6f7946257a
9a5a4cf246360000404220caf009ad02a57a48feb8d64d055509e9a81edba8d3
25e442cfe75e006a52000620b373fea9a31778be4dba6db03e38630c9e61e7a8
98f42cc5cc7be6ee87451ef5
```

A.4. Sender-Authenticated Messages

These vectors exercise the use of membership proofs to authenticate signed MLS messages. For each case, we provide:

* cipher_suite: The MLS ciphersuite.

* message_type: The type of sender-authenticated message.

* sender_authenticated_message: The encoded SenderAuthenticatedMessage<T>.

```
cipher_suite: 0x0001
message_type: "PublicMessageProposal"
sender_authenticated_message:
  20fe79a17d828b2f3eff2bd8b080c6c5fd27608223c990e663b0adeba3552a6d
  2a000000000000000201000000000002000100010001200309c7e25399293e95a
  8fb9cb2aa4c4802eddf31d18beacdd4a47353852f55c2b201400ee26cfbfc469
  cbac8fa119646f34713111adc7b08c787d21a069d9fcf603208a249f4b84c202
  2b22d92980a55598e3a1d8ab3795d2746446e3454b4b678b2b0001206a83e13a
  f79e11e0ba9dca3f1ecc1b115a18e205f89ee5df50948997fa9bc1b40200011a
  aaaa000100020003000500076a6a000600048a8a00080009000a041a1ababa02
  1a1a0a00010002fe00ff00caca0100000000000000000fffffffffffffff0c1a
  1a097a957520fa6ac3d1b64040524a42ec161d19a988d8045a1de673d3ead341
  11cd410ba04ff732fd56687ed6a7c55f2ba0debba59d365347498ab2099bd833
  e881aaca8d5fc32fe3f9d371070d2a2a0aa9372607772f7b3a7a0b40401ed23c
  72d2a31f5bdff39cf1617fb0295390484fe218b5bc3985b3cda312848dca5d2f
  a9639cad6c816b1c2844a0f68313edc33e77f43ca53d158066ab4b8a0a404042
  b8d7b64aa300d552736d03cb0f7007f9e9802b931b5bca76eab3488124cb2fcf
  32e4c9de79e1a168ecec467e5e9a9b1130147a8a187b5d55c8e98725e7010820
  e91d4d9ab60ff242a34e56f829e3e7f8db3df35db6071be490727d583ace1a1f
  0000000000000004410101012 0fcd9b75368fe537c0b250253545fa994240a27
  a2e30dd21e9032891b5cd0d53e202a47d26b3625a55a8ebde2ca5c85b195a98d
  e6d6179ee1c015bb2f86ab420314000120eede2b9dc21d5a8927b1c00d0fa88f
  99d2d66ec30c601c72704b53700833979c0200011800012a2a00020003000500
  0700065a5a0004000800090000a045a5aeaea026a6a0c000100025a5afe00ff00
  aaaa0100000000000000000ffffffffffffffff135a5a106dc76a6abd4b645185
  9fd82cabab2123404079a68373d838e6819ea93334c9c82bfb4387242c99f50a
  82c0c6d7df487ada3650d36786440733b3bd877e1f742a9abebcba4b1cd97117
  4a48ff24e75b948b0100004042205c559849bce6431f9db48e0acc0cdd278898
  f83a3827b02b7dea4e157b6cf9f520f8db898993af1dde0a3f5410aca1d76b99
  dd44542586782e0d47a801fc3db230
```

```
cipher_suite: 0x0001
message_type: "PublicMessageCommit"
sender_authenticated_message:
  20fe79a17d828b2f3eff2bd8b080c6c5fd27608223c990e663b0adeba3552a6d
  2a000000000000000201000000000030001206251d9705904845b0aa52ba71b
  a071c0313e4727cfb4a56916c654e3b4fcef6c202a47d26b3625a55a8ebde2ca
  5c85b195a98de6d6179ee1c015bb2f86ab420314000120eede2b9dc21d5a8927
  b1c00d0fa88f99d2d66ec30c601c72704b53700833979c020001160001000200
  0300050007000600040008 9a9a0009000a045a5acaca028a8a0c3a3aeaea0001
  0002fe00ff0003202a6a0c4c994902aab90352efc1acab1abaaa2a549c51aa3b
  e200876786778ede0fcaca0cf3bd75cf653d73591f0d43a44040cc07dba4b5fa
  8be01668326cddc9fcd168572ae87582145bde480a83e0bed418cb6eed1917c9
  fe317ff9b706e1e40af3d3bc9a1b8b939ed9b3b13f7d1ef2ea0e40ea20d9d847
  0fb1daebc4df692532d746b6c664777daabf4ef98b5b40bb6bc1d96472405220
  07fcb2e5fed1287d40573c02150029ecb74ad6bbb31b3e6ac9b7b8379de56d7c
  3083db086cb982bd0a7e85b58cf521da1e0c19d75659bfebd11d1073b220991b
  453d7696e0e8f7a7239bbd074dbf74063620a80e8bd7bbdfa00b97f8d3e44d52
  d2b598580ac67b3a265971b7724085a0710040522024b3385cc44d1996e06ba4
  4806f36f886dadc325ed53a563222e523b2d1ecd73304b85072ba3f4e0f6b699
  27821a2f875aa86a833bb598aa64b206c011d7c8dfa3c877a7de5e587f8fe553
  2f81d157cf4440406e2eaf5581c15ab98d27f4a37290e3b0b7095eec68cf6d5f
  ebaa9021ec7613afdf42d04507eb3323f6c7e1fe3f69f07714af5d3069542820
  3975757d22eaf70a200ca17a28db1ebb20479ac24dade6a17a598f8379ebcbba
  a939272bd80dc5ff18203f0f65d78b5d82f9dc8648457e752fb23dcad5fc4502
  8a31e7ddcf9884c6c1940000000000000000440fb010120fcd9b75368fe537c0b
  250253545fa994240a27a2e30dd21e9032891b5cd0d53e202a47d26b3625a55a
  8ebde2ca5c85b195a98de6d6179ee1c015bb2f86ab420314000120eede2b9dc2
  1d5a8927b1c00d0fa88f99d2d66ec30c601c72704b53700833979c0200011600
  0100020003000500070006000400089a9a0009000a045a5acaca028a8a0c3a3a
  eaea00010002fe00ff000100000000000000000fffffffffffffff0fcaca0cf3
  bd75cf653d73591f0d43a4404054704c131d68f29779db771ccdce5f9fd557a7
  506ff7b1dc6fd6e4486b4d8bd666a4ddf74bc749d99f84862ca22d7b27f648ac
  dcfe3be22ba98bb9b8ad849f060000404220711423a63ba695cb333836e8eb1e
  da2a17c64efaff67e08c16b4f0f4cce120182093374382089 18a6ddf7306b65d
  33718f891d8c9b433eeb544e5dc4ccbde2c23c
```

A.5. Annotated Welcomes

These vectors exercise joining a group as a partial client using an AnnotatedWelcome. For each case, we provide:

* cipher_suite: The MLS ciphersuite.

* external_psks: The external PSKs used to decrypt the Welcome, if any.

* key_package: The joining client’s KeyPackage.

* signature_priv, encryption_priv, and init_priv: The joining client's private keys needed to process the Welcome.

* annotated_welcome: The encoded AnnotatedWelcome.

* joiner_leaf_index: The joining client's leaf index.

* epoch_authenticator: The epoch authenticator derived by the partial client.

```
cipher_suite: 0x0001
key_package:
  0001000500010001200afba03cade48049231ba968c40cbb84b8083bf648c8eae
  5b60cf085005e947262069c5ca9ffe9dc396483edb69b1272d268fccd9ea9bbe
  e7fddd97c4370d26202d20a9f89b5a38f9c2a0be1f41fac893e2073c138d1d96
  8dafe71f04cee5019e3064000120cbc2f7b29a6e6443ea3b0d379a9c3358856c
  62d244083bb9d24ce58e6d8416b80200011600010002000300050007000600004
  000800095a5a000a04caca5a5a02caca0a00010002fe00ff005a5a0100000000
  00000000ffffffffffffffff07caca041a702e1140404b16d6959680243ed870
  ec5b052369a4bb90420f0243cb87810d699e23a5060ca56d78a366c29aadc9fc
  c41bbf65a85e2caf490403aefb670bf692f0965b1d0d10aaaa0db53adab45a8a
  4ee450c110cc744040a7758be0dae015090ff5a072b08ef30b472b57bfdad50d
  e373fa6eae857b451e19dbc045bced3ca47012ca50eba32292edded7b52d8b7c
  0f1c8cbe070783470b
signature_priv:
  118e562858f41a3ae69774c2470055c2598b3e251a237f57a8af90447ecde7e9
encryption_priv:
  ec7d424df7c16b8cd490fa98496ff5ebdb488544bd2c1795fcb9f50f39eca9da
init_priv: e3db009c0aed0c38a17147cb3c4e18319d2e59a8d155f9a3e700cfba892db24d
external_psks: []
annotated_welcome:
  0001407620b19d4b94dedb07d00a694fde115fe7a321623ba11d3ad5ab6f34b8
  f06b642f602037830d9198a92fbbab54445ab4ff9199a5b28969645c901c3668
  e6333a11db1333f50e5cc276f66b816cd6c5edd11d5e18b1fa4ff9c15d29631a
  e51fe903894f05028d4d438e7837001fe0c7807e27b49135b78a40fa7d9ef820
  c6cd25be5858b212742fe433d39426777364a0c63cbd8ea3624c8b8878d2ccc2
  5321eaf87e145657dae27ba18ac72be52a222c35ff26d1fcf214210440b68453
  e20db0c846e7fa10b12f6a922a097d4b568952ae8c8b8af70eb5f5eb71df1869
  5d70f439c80d79bba9097eabe822b820a09691893994acb97a3dcc38245a90b1
  a15957823162e1399416dbb8a9fc4e8bb5e522ab524c2066aebc3ecd6923b645
  0d78806d173073751e004c457498e681c4720f3a772e4256f7a6182ba5de217f
  bad4735358fe4282832dbb7da93dbddaedaa97091a48479d7b4f35a748384a83
  74f5e8e7fc6e3faa00b2aa30b9c0e650a131218939f900000000000000440ed
  010120dbb1d9404971b5bd6490eab26921fa1a7727aa391fbde2acf522eaa7f0
  cd362020853f9fe1c5479a2b24f96f716443437391d4d92ca8e749c9d2bc57fe
  5e44961f00012039d868b71f650c674a2deca847e816ab42c965343890250223
  06a0db30cb41f4020001160001000200030005000700600043a3a0008000900
  0a045a5a4a4a02baba0a4a4a00010002fe00ff000100000000000000ffffff
```

```
    fffffffff034a4a004040badead157f507ab974920f8e6ddca82109a2763c1a
    37e5671bc239fccf5d423125d6ccdde2799d6a3b4f482562cf0d04a807a21a4c
    f8177c21fcf0f0abce7d020000404220ea58558304edb88e8f396f3b28dc306f
    9c007471f968bf8bd6611ab381e7eab5207c668881e92bb6e98a8709a042111a
    5f452632b0d9680372964ad38f1d406e5b0000000020000000440f101012069c5
    ca9ffe9dc396483edb69b1272d268fccd9ea9bbee7fddd97c4370d26202d20a9
    f89b5a38f9c2a0be1f41fac893e2073c138d1d968dafe71f04cee5019e306400
    0120cbc2f7b29a6e6443ea3b0d379a9c3358856c62d244083bb9d24ce58e6d84
    16b80200011600010002000300050007000600040008000 95a5a000a04caca5a
    5a02caca0a00010002fe00ff005a5a0100000000000000000ffffffffffffffff
    07caca041a702e1140404b16d6959680243ed870ec5b052369a4bb90420f0243
    cb87810d699e23a5060ca56d78a366c29aadc9fcc41bbf65a85e2caf490403ae
    fb670bf692f0965b1d0d0000404220caf009ad02a57a48feb8d64d055509e9a8
    1edba8d325e442cfe75e006a52000620c4aa8eac612c4528d4fd084bb8817052
    1e654d5f039b7189480f7ee3040507d4
joiner_leaf_index: 0x00000002
epoch_authenticator:
    6dd7b6ec4e3dcec3281b34001f81efed6bced01f853cd4e5bb7e52e112f347db
```

A.6. Annotated Commits

These vectors exercise processing commits as a partial client using an AnnotatedCommit. For each case, we provide:

* cipher_suite: The MLS ciphersuite.

* state_before: The partial client’s state before processing the commit.

* proposals: Any proposals referenced by the commit.

* annotated_commit: The encoded AnnotatedCommit.

* tree_hash_after: The tree hash after the commit is applied.

* commit_secret: The commit secret computed while processing the commit.

* epoch_authenticator_after: The epoch authenticator for the next epoch.

* state_after: The partial client’s state after processing the commit.

```
   cipher_suite: 0x0001
   state_before:
     confirmed_transcript_hash:
       821ed26b3cf58141dc3b72b111971c3bb0a0ae3c9d12393c693738b580f1cda5
     direct_path_secrets: []
     encryption_secret:
       5ce258a673dde89a50401ff30fcef15ba9b595c33c80e7bec39789a62966217c
     epoch: 0x0000000000000002
     group_id: e3ca77d4487c7eaa03c2644ad271df588ee277b4ba489cbd1ebe57ea337a0c44
     init_secret: bee4f048eb68d6bc2a9428924c2cedf23dcb572f3b0820842d2c4689bf64482f
     interim_transcript_hash:
       bb5cb17c25dbad51292a2490c948e5434bb0e553de7a0c667dadcf8ed1b71860
     membership_key:
       135a9227dd16eb9f0e8fa98d01d910b9f497a1022c9996a0d93404bb2d3d928d
     receiver_leaf_index: 0x00000002
     sender_data_secret:
       b811cc5f5d3d4ee2effc434d0174b75a8fdfc3a2b926a2381dc1e170b3ca8169
     tree_hash: f96b46bc290fd275cc22bbfb2ef62ae10f6c04c0689dcd9bc1fb6de821e820c0
   proposals: []
   annotated_commit:
     0001000120e3ca77d4487c7eaa03c2644ad271df588ee277b4ba489cbd1ebe57
     ea337a0c44000000000000000201000000000030001201d76905027cef874e4
     f933f1ad5b29fa59a12acc41bb87977e55c5231f88660120ab729634d3e88256
     626dcce845a8b7cf4b7493d3edd328549f9414841553879700120ca0a604d9d
     b20c7611d4f302753db8b98509708e87f7658135d177e9649e97fa0200011c00
     010002eaea000300050007caca00060004000800096a6a7a7a000a02caca021a
     1a0c0001aaaa00024a4afe00ff0003202ef022d23470a8e0255d86e8d079ea86
     1c8612560eed0acf6f4a2445a9ab989908caca0509afc08cc440403fdfe52dc6
     8fe8d54d6ebd3d79fc02624ba38ea25b79811761728ca0961969f33046aec24a
     751c4c1590975b24dc83668e9d171bda6feac5eab53925e452df0440ea20ae87
     fc74bdf7e50b5d2ebb0a084ac78f8c9b7e4aace51a2321643814cc83bb3d4052
     204384562de0851e0fbbfa998931fa3d982bcf0d2ab28415afc2b73d9db9bc9b
     7d3083b6b258a74d67130a28d0d00b8c6d97b3c7eda0c20479a4e8764bc28204
     ff049ac561c071610dc9122bc002a550de26202fec807d86e4df88b9d91957e3
     522df451d5a4cb2bbae1d46ccb44708796141740522031 4d566ad22c44f803d1
     0e2056ee280558a56bd8a3555fc84905cac8bb6bfd79301221c8452f5b0f8722
     721ef9732f05f78bdeae3bb8d68c715700f22be4091a5e25eb91accb3f4a80b9
     2399044ddae45840408368c886434f1c1ec68b41d1880e25d339f3ebceaac534
     46383005ec9d2882595050a6028d5e7f875ed6fac7c6b63ef623ef9c62d35c57
     83500d3e7d5eb9c80420511c80dd4348daa10bd38c473acbc18ac56fe159aa2f
     94f02344b5b03bd8e5f420eb178abbd7da0c216f6b53ec42a8ffab241576b8fe
     2a4fc9fd97592488988a8f0100000000000000000440f801012063c37d0b84049d
     52defec2e4abde40bad3c9c4c24b4ce1fc3f230c8064f8fc5420ab729634d3e8
     8256626dcce845a8b7cf4b7493d3edd328549f9414841553879700120ca0a60
     4d9db20c7611d4f302753db8b98509708e87f7658135d177e9649e97fa020001
     1c00010002eaea000300050007caca00060004000800096a6a7a7a000a02caca
     021a1a0c0001aaaa00024a4afe00ff000100000000000000000fffffffffffff
     ff08caca0509afc08cc44040e02b8971e45107c5255a7247c786402f285f3fa7
```

```
    1d21af1da37b9f7e2a4dce2c0325c3a688681a3875590df380f5b2812786d9cc
    0f17f34489b6c10572f1d00e0000404220b990565226fb7edd02c7f845467862
    8c2b7f2bb2d96a742d07a2f5a0738b6bef204142c73a864fda6cd1df893a39a3
    012d911aac84aec5c74af4be8419afb373f5201bde7445375a0e521aaac260c6
    87441f246c54c5d820b0c3a9b901f7555e773f0100000000000000000000000004
    41710101201d76905027cef874e4f933f1ad5b29fa59a12acc41bb87977e55c5
    231f88660120ab729634d3e88256626dcce845a8b7cf4b7493d3edd328549f94
    148415538797000120ca0a604d9db20c7611d4f302753db8b98509708e87f765
    8135d177e9649e97fa0200011c00010002eaea000300050007caca0006000400
    0800096a6a7a7a000a02caca021a1a0c0001aaaa00024a4afe00ff0003202ef0
    22d23470a8e0255d86e8d079ea861c8612560eed0acf6f4a2445a9ab989908ca
    ca0509afc08cc440403fdfe52dc68fe8d54d6ebd3d79fc02624ba38ea25b7981
    1761728ca0961969f33046aec24a751c4c1590975b24dc83668e9d171bda6fea
    c5eab53925e452df04010220ae87fc74bdf7e50b5d2ebb0a084ac78f8c9b7e4a
    ace51a2321643814cc83bb3d201185e5abfa5e37c22f93912c8cb4149837f328
    1ffa980891df4b3c59c393d219000102202fec807d86e4df88b9d91957e3522d
    f451d5a4cb2bbae1d46ccb44708796141700000404220b990565226fb7edd02c7
    f8454678628c2b7f2bb2d96a742d07a2f5a0738b6bef204142c73a864fda6cd1
    df893a39a3012d911aac84aec5c74af4be8419afb373f5000000020000000441
    1401012098460b770a443bd6120967e2774c3c2a59c94d6e58bc81644e7bc05d
    f9a1360120d7b60c76cb013ecdff92ef08ef21f81e449a71971986d32b9f9f74
    b106481c1f00012078d777a3a789d2ae1c7a242cf36acf119fa15fdee7c09ece
    39a26a19faf4849a020001160001000200030005000074a4a0006000400080009
    000a04dada7a7a026a6a0a00010002fe00ff003a3a01000000000000000000ffff
    ffffffffffff06dada036a482e4040b0eb0b93c18de78a0e7d424c563de186c8
    39a5f23739cf1308d96c942a88a9077d21df2c2f85a9bbc46be586b8a5012458
    a996186943fa7ca3c19ee15696bb03000102202fec807d86e4df88b9d91957e3
    522df451d5a4cb2bbae1d46ccb44708796141700000404220caf009ad02a57a48
    feb8d64d055509e9a81edba8d325e442cfe75e006a520006204b805219410102
    9dd4123cb7859f236edb375a68c94750d0ce665d552f4e6244
  tree_hash_after:
    1bde7445375a0e521aaac260c687441f246c54c5d820b0c3a9b901f7555e773f
  commit_secret: c5ebf7b193c389b914fc9df28c84b845ec134e65a4cc8eae3c47ba984e8dca92
  epoch_authenticator_after:
    e194515ecf0193e28f8c56c5865608a211e8f4ff07c7cc298d5c50f2a39e6aca
  state_after:
    confirmed_transcript_hash:
      688b7ef507501bfea2dc3ccf71497650e54c7b47e01fd5ad0d94960c073cd9eb
    direct_path_secrets:
      -
        encryption_priv:
          0762c3075664239311a812a999733e87db7297b9f23e4ea79c37d27f50143939
        node: 0x00000003
        path_secret:
          e635ee4566b2afd1fab148fdc1563cf8694bf8a48eef064be09dad7861f87023
    encryption_secret:
      93f27aff9c6ee1a4383f0a749cdd9b9a47a10071c0cf406da1b2289f7fa110bc
    epoch: 0x0000000000000003
```

```
group_id: e3ca77d4487c7eaa03c2644ad271df588ee277b4ba489cbd1ebe57ea337a0c44
init_secret: 3383f7965265d3dc27c5c0f5f2f185b69efa746368b43a54ae90258590dbac11
interim_transcript_hash:
  09d3b700df4130ea458cefa322e48431b99e9113f0c9a6766417486d25cea027
membership_key:
  8b97e308c6c56aa296bca70847eff9814e4c878b28fe27dd5d0f72e88b9ea9e6
receiver_leaf_index: 0x00000002
sender_data_secret:
  8e415bd5e07fe34ab923a08bbf60f2b80a00b8a2eff0f3b9a7b72c7209f1de0c
tree_hash: 1bde7445375a0e521aaac260c687441f246c54c5d820b0c3a9b901f7555e773f
```

A.7. Partial Passive Client Scenarios

These vectors exercise a partial client joining a group and following several epochs without storing the full ratchet tree. For each case, we provide:

* cipher_suite: The MLS ciphersuite.

* external_psks: The external PSKs used to decrypt the Welcome, if any.

* key_package: The partial client’s KeyPackage.

* signature_priv, encryption_priv, and init_priv: The partial client’s private keys needed to join the group.

* annotated_welcome: The AnnotatedWelcome used to join the group.

* initial_epoch_authenticator: The epoch authenticator after joining.

* epochs: A sequence of proposals, annotated commits, application messages, and epoch authenticators for subsequent epochs.

```
cipher_suite: 0x0001
key_package:
  0001000500010001202 4b2e6c9cf0141917cfc8fe84c7add7dbeb67d5d95e477
  01038005733b2292252037c89d463611a307df9e98b2df32daf0a4aa0a32dca0
  f590b75c9534372f521f20e349c4ab357225bb6fdf57e5d2b53aac7a7afcf009
  6036ea16e7a0f6208265cd0001206b47045927b857930c3fffe23059f96d1111
  bb84d3fb5313094eccfb62e8522a0200011c0001000200030005caca00077a7a
  00063a3a00040008dada0009000a04baba0a0a025a5a0aaaaa00010002fe00ff
  0001000000000000000ffffffffffffffff050a0a0206334040f513ed0efdbf
  49964e5ada1b63e5b61c5d33e43156ace19d8979e4a95c748ffd328cc8a096d9
  21b4317b9bd3282b996a9b0272f5194e8f7dc7b151de5101d308133a3a10fac1
  9abfb26f277c199ff0feab4ea33a40407dc5ce16e816bbabf724b4b3d6f88624
  9b0da9283b06f3ac41a235811b9c91cd0ca6f91a734a11e805ae1d3b24cc25fc
```

```
    a064ddf390a9fbe8a2d62f889cdde209
  signature_priv:
    d61c88f757d1730fed551a53e4e8662dafd87fe426cbec9b1693bc3e325526f3
  encryption_priv:
    f7e9774e3fa3e5d0b79ff2804cfd272e8138e80e6045efb26b422491d2b47238
  init_priv: 6179807a85593e612f7dcf05f94ee1e6769377ea9b12963144953a3ffdeb0d07
  external_psks: []
  annotated_welcome:
    0001407620e7b00d56abfe9dc50fe5c7c2de311687737afc21cbd683d8b60fae
    c3ff83a77f20653f1cfc8adc7e2f20268c287aa8532332368ff652cbfa8d37a3
    d6d2073de45e337824be17f4af25de3ba84c4e945d7bfa28ed58ef3a5b93368e
    4371d2612ce53b4e62763dbadb0475d477ce4fd70905598c1c4240ee14e1fabd
    4defa7804423f73235e688a10a3a3df0d69f849ff1b941156dbb0258e641b0e8
    512dda2670afd1c11e32a39ca986fe771bc356a6b8bc03c512373c10869bb68e
    a8997cd913d6ffc4cd44bd8d4589920f2ebb8b1f491705253a370d8c36922978
    09d66423010e3d734a03c2a9cf93cea688615f67f0534ab81657d40368e6a468
    d1ef13cf29347f1c0471b8195b67d7b091fb7d6b7f9da1faaf820c243e401957
    31903d241e1585dc6f3fb55085b6725f6f4bc9f4b2cb24e69ff5d6303ebac31d
    4a974b6c95c8fc2ca46f0f82e7f9d4f3fab53b9a74839995929ef0193d099285
    ffba6ed22503b23de5de00000000000000440f001012077277ef2675c808ddd
    82da643ffba9c41f8b7affa67aad17bbdda66c6ccb9f1f203e0ee34d110f8d4b
    f3ec009497b5d122376470c5ffcadbf1d126eedbcdac527700012052f9a4b072
    ea45c8f5e78c63c9c3613aa111d31d827336594133 86f80f97d0a30200011800
    0100020003000500070006000 46a6a0008dada0009000a044a4acaca02dada0a
    00010002fe00aaaaff000100000000000000000ffffffffffffffff044a4a019b
    40407b000877778dc610a1fd6823a7145935a186ff1c27ca0eca091f93d0a422
    e6505523fb0a0e7d7d0013954771ffd2da1768aed0df94ec2a330fa2d6d4398b
    210500004042206fe0ff831a2869776d762948f50febdb765cf8c09d30214147
    29b1779625edd020dfb7450d78d3ca9016f4640e6e5f36ce54cc10e8b407a53d
    8a1016e50093d9b3000000020000000440f501012037c89d463611a307df9e98
    b2df32daf0a4aa0a32dca0f590b75c9534372f521f20e349c4ab357225bb6fdf
    57e5d2b53aac7a7afcf0096036ea16e7a0f6208265cd0001206b47045927b857
    930c3fffe23059f96d1111bb84d3fb5313094eccfb62e8522a0200011c000100
    0200030005caca00077a7a00063a3a00040008dada0009000a04baba0a0a025a
    5a0aaaaa00010002fe00ff000100000000000000000ffffffffffffffff050a0a
    0206334040f513ed0efdbf49964e5ada1b63e5b61c5d33e43156ace19d8979e4
    a95c748ffd328cc8a096d921b4317b9bd3282b996a9b0272f5194e8f7dc7b151
    de5101d3080000404220caf009ad02a57a48feb8d64d055509e9a81edba8d325
    e442cfe75e006a5200062055a6ca955bbc02019e12b2c11689623550468d6f41
    0ee841469352fd605953cb
  initial_epoch_authenticator:
    797749a338c0a57abb4df3a52494e7ad0f12d3e576964b20546e35595f9dd015
  epochs:
    -
      annotated_commit:
        00010001202af8e1a35853f84a78f3c49ea2656f505ae35132fd240fedd61a7b
        6084ea16e2000000000000000201000000000003000120774239e9c752940020
        4a47df0089ffe30294f59b7695b80668736aab6cfa073c203e0ee34d110f8d4b
```

```
f3ec009497b5d122376470c5ffcadbf1d126eedbcdac527700012052f9a4b072
ea45c8f5e78c63c9c3613aa111d31d82733659413386f80f97d0a30200011800
0100020003000500070006000046a6a0008dada0009000a044a4acaca02dada0a
00010002fe00aaaaff000320b8bac7f8019aca2a6b070f62a8654930355076d1
ca75971e93e0d9a1bb9af5ed044a4a019b4040f8ab715b478e846bbf35620d9e
2473bec1c18a12ebf0231752e38bc6c206ba8e78d6c6bac62575e621bb79345e
258834a297159b08dd824a35571221ab1c6d0a40ea20b7978bda81202ca30468
334be6c124f1fee93799c8ab3a2bdce7e9f7c2a62c5e4052202da9b610227897
3042423018fe787de8b05d7fdbab056e3fcf881e95f498b637305f4f7be7fe38
b2785bbc65753bb555f03758b2b1ea665cfbf8b81c1ddd7be520c50a16db16cf
d46033e892086cbf139720d0dc8105da6dcef361247baf264d6a4eb88f954617
70063cd069971c32dec62040522049855d45d8ee3818fe9834bd4714faa29cb4
b8fa5a19c4b0b2ea82220c27bb563064b1e1df2cd5d33bd2c71a1ee761ef16d2
87c6233d8d000f05ce86c19b2e492d080c7867b7b4981ae67efe5dae48a37940
402a3c495b8a278f9210876c14c227df304cff9ca1ed215437daec966b33da87
b6efb048820cb6814f9a568e8c090e88ce32270c7acb6d3eb7e7a244efc8a01f
0920bd5a83c5dd82cc18e645867a5d1eb2e26af09c6a61ad02a590f3acfe41cf
f2ff20f42dd4481d8dc003aedc87dd5ed5368de1f3cf8f9e77208f094c776419
9ed824010000000000000000440f001012077277ef2675c808ddd82da643ffba9
c41f8b7affa67aad17bbdda66c6ccb9f1f203e0ee34d110f8d4bf3ec009497b5
d122376470c5ffcadbf1d126eedbcdac527700012052f9a4b072ea45c8f5e78c
63c9c3613aa111d31d82733659413386f80f97d0a3020001180001000200030 0
050007000600046a6a0008dada0009000a044a4acaca02dada0a00010002fe00
aaaaff000100000000000000000ffffffffffffffff044a4a019b40407b000877
778dc610a1fd6823a7145935a186ff1c27ca0eca091f93d0a422e6505523fb0a
0e7d7d0013954771ffd2da1768aed0df94ec2a330fa2d6d4398b210500004042
206fe0ff831a2869776d762948f50febdb765cf8c09d3021414729b1779625ed
d020dfb7450d78d3ca9016f4640e6e5f36ce54cc10e8b407a53d8a1016e50093
d9b32074d7afe185c006ea8742578de827102ed83478ef2089f44078af101d0a
2d617701000000000000000000000004416901012077423 9e9c7529400204a47
df0089ffe30294f59b7695b80668736aab6cfa073c203e0ee34d110f8d4bf3ec
009497b5d122376470c5ffcadbf1d126eedbcdac527700012052f9a4b072ea45
c8f5e78c63c9c3613aa111d31d82733659413386f80f97d0a302000118000100
020003000500070006000046a6a0008dada0009000a044a4acaca02dada0a0001
0002fe00aaaaff000320b8bac7f8019aca2a6b070f62a8654930355076d1ca75
971e93e0d9a1bb9af5ed044a4a019b4040f8ab715b478e846bbf35620d9e2473
bec1c18a12ebf0231752e38bc6c206ba8e78d6c6bac62575e621bb79345e2588
34a297159b08dd824a35571221ab1c6d0a010220b7978bda81202ca30468334b
e6c124f1fee93799c8ab3a2bdce7e9f7c2a62c5e206d65d28169a4b8ec000867
9dbf8b30e7a736f06c74840da2bf9a688762d320d100010220d0dc8105da6dce
f361247baf264d6a4eb88f95461770063cd069971c32dec62000004042206fe0
ff831a2869776d762948f50febdb765cf8c09d3021414729b1779625edd020df
b7450d78d3ca9016f4640e6e5f36ce54cc10e8b407a53d8a1016e50093d9b300
0000020000000441190101203 7c89d463611a307df9e98b2df32daf0a4aa0a32
dca0f590b75c9534372f521f20e349c4ab357225bb6fdf57e5d2b53aac7a7afc
f0096036ea16e7a0f6208265cd0001206b47045927b857930c3fffe23059f96d
1111bb84d3fb5313094eccfb62e8522a0200011c0001000200030005caca0007
7a7a00063a3a00040008dada0009000a04baba0a0a025a5a0aaaaa00010002fe
```

```
      00ff000100000000000000000fffffffffffffff050a0a0206334040f513ed0e
      fdbf49964e5ada1b63e5b61c5d33e43156ace19d8979e4a95c748ffd328cc8a0
      96d921b4317b9bd3282b996a9b0272f5194e8f7dc7b151de5101d30800010220
      d0dc8105da6dcef361247baf264d6a4eb88f95461770063cd069971c32dec620
      0000404220caf009ad02a57a48feb8d64d055509e9a81edba8d325e442cfe75e
      006a520006205bd4d7bc424888cbebe5da155008e25e1b8dc986835abee7acb1
      286cfabdb377
    application_messages:
      -
        00010002202af8e1a35853f84a78f3c49ea2656f505ae35132fd240fedd61a7b
        6084ea16e2000000000000000301001ce087fa00006a307707933f4fa91ca3d4
        e85e3e664f2dfec88d2b4d0340732f1c585599e650527d25a56571a5f4bf27f3
        670d23dc583c9dbb14cc832926ae09e4f2d076697a75c206622f08e977b20186
        5a0ebb357ccc80b8a55e8fbc68437ac9524132ea2dbf001a2ecd36896830b68d
        24c58739d31b203549156728701315a6a4be3d5f65b5452a07723db5464e33d5
        7e0000000100000004416201012 0b8ee593dbb1112f974c4cbb4978440123612
        2102feb656b5e1df364810e1071f20d02d3c2f629e10e39aeb304a38af3a4d83
        029591345bf72aa53fa6b2dec1a8ab000120764f19155935995dc0e06a8df057
        049b871d094555320a35e7797dfdec200c790200011e000100020003000500 07
        000600047a7adada00085a5a2a2a0009000acaca04caca0a0a02dada0a2a2a00
        010002fe00ff000100000000000000000ffffffffffffffff08caca05f1d19dd7
        ce4040c8a448335607f0521196510afb549aaf9e3e7cf07810f0dd854159fe23
        84983a28a629948aec5e42b1d164ff6d1bd94dd5a98477c0a4e8f79288323693
        77120a010220b7978bda81202ca30468334be6c124f1fee93799c8ab3a2bdce7
        e9f7c2a62c5e206d65d28169a4b8ec0008679dbf8b30e7a736f06c74840da2bf
        9a688762d320d100010220d0dc8105da6dcef361247baf264d6a4eb88f954617
        70063cd069971c32dec6200000404220b9c09c54dcd15b1035dab218ecd7dfd6
        af7edbbbfe810db7319a57412b5daae320dfb7450d78d3ca9016f4640e6e5f36
        ce54cc10e8b407a53d8a1016e50093d9b3
    epoch_authenticator:
      fbf49347f9670a235ce818073593a9d8399d412bf483b54e2d7fc0038aa1897a
    proposals: []
  -
    annotated_commit:
      00010001202af8e1a35853f84a78f3c49ea2656f505ae35132fd240fedd61a7b
      6084ea16e2000000000000000301000000000003000120500bad2bec440409bf
      9596b093af989b78da891ae6d29f53e73cf6f80c9aef53203e0ee34d110f8d4b
      f3ec009497b5d122376470c5ffcadbf1d126eedbcdac527700012052f9a4b072
      ea45c8f5e78c63c9c3613aa111d31d82733659413386f80f97d0a30200011800
      0100020003000500070006000 46a6a0008dada0009000a044a4acaca02dada0a
      00010002fe00aaaaff000320bd70e4afd05e4ab967b8ec03302a2e8126a62ab1
      940b90db10b4bbc4fe80ff8b044a4a019b4040f5a66dd4ac1f0bd2175f559c86
      0ee6090cb1c376928d5bf38e4c999d837adff13466239322454a4f8d03a423fc
      071263111ae536ea7c6b03a2f595f231195d0940ea2006e43355bb863b9afba8
      e45ce37a3ca875b0a5a6539597a1a3f1d368141a164f405220ebdf7d6a24269b
      7aa90c07058a58f39d799a39397f7d59104e6754026b28533130fae24664dc50
      f357833cffd9a1850fe72badd876164236535d5b88399ef44915685ec526ca32
      7d9491a39d685f9077bf20837b76f30e3dcd620a7bb83a0cb3d03aadb1bae436
```

```
      73778d3ec4dc7e0e1438674052203fe91c2566da8b7f60d1b84849650f147595
      be7f46c8211a5de41c84cf5d2242302e167cf1f06820a4d0094358490198f7e9
      bc8275fd13b6f3f105a8cbd73cb4892a423344087beb4963ecd7619b789cd740
      4045078cee6d9df0aac357fea8cd375ce72e82ada6179eea26a7821fa36b120d
      6f391ad5484691d77134740fc547d3a2d2ff5cdb20bf1d9de43d77da576c4723
      0420fc2f3a0434ab485d87d529b34a5e9171c76af65fd51197c6a6a660df3dec
      6c2e20094d3dc4212056ccfbcb510706e73afe4b4c8034efec6a31e5ce095831
      e623dc0100000000000000004416901012077423 9e9c7529400204a47df0089ff
      e30294f59b7695b80668736aab6cfa073c203e0ee34d110f8d4bf3ec009497b5
      d122376470c5ffcadbf1d126eedbcdac527700012052f9a4b072ea45c8f5e78c
      63c9c3613aa111d31d82733659413386f80f97d0a3020001180001000200030 0
      0500070006000 46a6a0008dada0009000a044a4acaca02dada0a00010002fe00
      aaaaff000320b8bac7f8019aca2a6b070f62a8654930355076d1ca75971e93e0
      d9a1bb9af5ed044a4a019b4040f8ab715b478e846bbf35620d9e2473bec1c18a
      12ebf0231752e38bc6c206ba8e78d6c6bac62575e621bb79345e258834a29715
      9b08dd824a35571221ab1c6d0a010220b7978bda81202ca30468334be6c124f1
      fee93799c8ab3a2bdce7e9f7c2a62c5e206d65d28169a4b8ec0008679dbf8b30
      e7a736f06c74840da2bf9a688762d320d100010220d0dc8105da6dcef361247b
      af264d6a4eb88f95461770063cd069971c32dec62000004042206fe0ff831a28
      69776d762948f50febdb765cf8c09d3021414729b1779625edd020dfb7450d78
      d3ca9016f4640e6e5f36ce54cc10e8b407a53d8a1016e50093d9b320f659d2c1
      c834bcbb021b47a12f71530b455c394de2f021c5f9635e28e27269b101000000
      0000000000000000044169010120500bad2bec440409bf9596b093af989b78da
      891ae6d29f53e73cf6f80c9aef53203e0ee34d110f8d4bf3ec009497b5d12237
      6470c5ffcadbf1d126eedbcdac527700012052f9a4b072ea45c8f5e78c63c9c3
      613aa111d31d82733659413386f80f97d0a3020001180001000200030005000 7
      000600046a6a0008dada0009000a044a4acaca02dada0a00010002fe00aaaaff
      000320bd70e4afd05e4ab967b8ec03302a2e8126a62ab1940b90db10b4bbc4fe
      80ff8b044a4a019b4040f5a66dd4ac1f0bd2175f559c860ee6090cb1c376928d
      5bf38e4c999d837adff13466239322454a4f8d03a423fc071263111ae536ea7c
      6b03a2f595f231195d0901022006e43355bb863b9afba8e45ce37a3ca875b0a5
      a6539597a1a3f1d368141a164f2072d43bb60525c3756df7cf9670c026608946
      80310c68fb938b0164de5552eb3000010220837b76f30e3dcd620a7bb83a0cb3
      d03aadb1bae43673778d3ec4dc7e0e14386700004042206fe0ff831a2869776d
      762948f50febdb765cf8c09d3021414729b1779625edd020dfb7450d78d3ca90
      16f4640e6e5f36ce54cc10e8b407a53d8a1016e50093d9b30000000200000004
      411901012037c89d463611a307df9e98b2df32daf0a4aa0a32dca0f590b75c95
      34372f521f20e349c4ab357225bb6fdf57e5d2b53aac7a7afcf0096036ea16e7
      a0f6208265cd0001206b47045927b857930c3fffe23059f96d1111bb84d3fb53
      13094eccfb62e8522a0200011c0001000200030005caca00077a7a00063a3a00
      040008dada0009000a04baba0a0a025a5a0aaaaa00010002fe00ff0001000000
      0000000000ffffffffffffffff050a0a0206334040f513ed0efdbf49964e5ada
      1b63e5b61c5d33e43156ace19d8979e4a95c748ffd328cc8a096d921b4317b9b
      d3282b996a9b0272f5194e8f7dc7b151de5101d30800010220837b76f30e3dcd
      620a7bb83a0cb3d03aadb1bae43673778d3ec4dc7e0e1438670000404220caf0
      09ad02a57a48feb8d64d055509e9a81edba8d325e442cfe75e006a5200062071
      f3bcd57435d50a2271035bd497ff1ad9b7e9ddb46df7c379f78092d5badb1c
    application_messages:
```

```
      -
        00010002202af8e1a35853f84a78f3c49ea2656f505ae35132fd240fedd61a7b
        6084ea16e2000000000000000401001c4c101e401044edcfc2c142cd5136b6af
        dbd8c3e83198f022c691110b40731154bebeb00bc796e5c3e346d9753c1382ea
        58340da25270fe039af65a77aee89e30ef0f0f0deaabd6ee50ef04e7133c67fe
        32ccb2f521e7a7f9fa14becc02b199fc81a9dfaaf11f918adf249a1628fe87f6
        e1d2472319c3fcc849e76126026d4d3e63345e82970152d575ea549378ba14f6
        c900000001000000044162010120b8ee593dbb1112f974c4cbb4978440123612
        2102feb656b5e1df364810e1071f20d02d3c2f629e10e39aeb304a38af3a4d83
        029591345bf72aa53fa6b2dec1a8ab000120764f19155935995dc0e06a8df057
        049b871d094555320a35e7797dfdec200c790200011e000100020003000500007
        000600047a7adada00085a5a2a2a0009000acaca04caca0a0a02dada0a2a2a00
        010002fe00ff000100000000000000000ffffffffffffffff08caca05f1d19dd7
        ce4040c8a448335607f0521196510afb549aaf9e3e7cf07810f0dd854159fe23
        84983a28a629948aec5e42b1d164ff6d1bd94dd5a98477c0a4e8f79288323693
        77120a01022006e43355bb863b9afba8e45ce37a3ca875b0a5a6539597a1a3f1
        d368141a164f2072d43bb60525c3756df7cf9670c02660894680310c68fb938b
        0164de5552eb3000010220837b76f30e3dcd620a7bb83a0cb3d03aadb1bae436
        73778d3ec4dc7e0e1438670000404220d0dc23625c7166511a78fcd1a5084fb3
        6f411f08cc6c366b38beaa88dc73400220dfb7450d78d3ca9016f4640e6e5f36
        ce54cc10e8b407a53d8a1016e50093d9b3
      epoch_authenticator:
        ad76f6c0ab7c49653b77ad47e53e35e9d4b0a5364341120bdcceabc62cf9c629
      proposals: []
    -
      annotated_commit:
        00010001202af8e1a35853f84a78f3c49ea2656f505ae35132fd240fedd61a7b
        6084ea16e2000000000000000401000000000030001205fbada517b298cf817
        8350796e001bf74231f74875bfa69d418935ca421cf130203e0ee34d110f8d4b
        f3ec009497b5d122376470c5ffcadbf1d126eedbcdac527700012052f9a4b072
        ea45c8f5e78c63c9c3613aa111d31d82733659413386f80f97d0a30200011800
        0100020003000500070006000046a6a0008dada0009000a044a4acaca02dada0a
        00010002fe00aaaaff000320f47274a5ca029cbaddd6200c6edffe6953673a6d
        fe14a374dfb2ddb48b2805d4044a4a019b404096888fa26228966af730b8e61e
        9d0f18f9132fff6783eabccf7169d3170ceff0d9ad3834ca52802420d1bc6831
        3908cdc1665f82fd3b8254b86721f0e7a3860640ea20ddeb878addd0fae32eed
        f8b875de7523399bee24174453f9e478cab2b5ce7e6b40522057aa2d1b8793b5
        d3099834ba5108970bd59297940efba6478daaf90c4fa1640130a05abaec867f
        c3fdfc5cedfce085ee91eaa2bcaa87ecfe0ca3e41128d273371c25479ca36424
        e4eb6aa6d128e9eb10ea20462680fd79ee53114f3f501e2ca4102172097b125c
        bfa8b399e89869d4a589394052202b4021afb50091a5633f0aa5312eddd453f5
        3bb00f0b3a58466ee14eb8e4e00c30129db91a5e79c80f4bff38ea1023831036
        53ec45e07a20a1a37d0975f57fe5a4c2ceaf17011b60194fd5a0e2c1af475140
        406e9f3fcff512ae75dc25fb489f9e5dac7cd1f6fc4fbec29bbb7dd8b9b1b636
        eea3b8f928ab949ce9c01319836052e0267cb5eb446130ffba6390cdc427ec4a
        0120bb20efcd286195b793bdab66b44a8da29228365b6197a968a4263d1884ae
        239c205691af015862f4066c657018c4b2b5c3fe81c944d5c30f31aee2ea92d8
        7dd928010000000000000004416901012050 0bad2bec440409bf9596b093af98
```

```
      9b78da891ae6d29f53e73cf6f80c9aef53203e0ee34d110f8d4bf3ec009497b5
      d122376470c5ffcadbf1d126eedbcdac527700012052f9a4b072ea45c8f5e78c
      63c9c3613aa111d31d82733659413386f80f97d0a3020001180001000200030 0
      050007000600046a6a0008dada0009000a044a4acaca02dada0a00010002fe00
      aaaaff000320bd70e4afd05e4ab967b8ec03302a2e8126a62ab1940b90db10b4
      bbc4fe80ff8b044a4a019b4040f5a66dd4ac1f0bd2175f559c860ee6090cb1c3
      76928d5bf38e4c999d837adff13466239322454a4f8d03a423fc071263111ae5
      36ea7c6b03a2f595f231195d0901022006e43355bb863b9afba8e45ce37a3ca8
      75b0a5a6539597a1a3f1d368141a164f2072d43bb60525c3756df7cf9670c026
      60894680310c68fb938b0164de5552eb3000010220837b76f30e3dcd620a7bb8
      3a0cb3d03aadb1bae43673778d3ec4dc7e0e14386700004042206fe0ff831a28
      69776d762948f50febdb765cf8c09d3021414729b1779625edd020dfb7450d78
      d3ca9016f4640e6e5f36ce54cc10e8b407a53d8a1016e50093d9b3208c3a8ee7
      ef1b2a39f5a4c0eb23db07f79df81b2789b2948923a64a25b8392c7501000000
      0000000000000000044169010120 5fbada517b298cf8178350796e001bf74231
      f74875bfa69d418935ca421cf130203e0ee34d110f8d4bf3ec009497b5d12237
      6470c5ffcadbf1d126eedbcdac527700012052f9a4b072ea45c8f5e78c63c9c3
      613aa111d31d82733659413386f80f97d0a3020001180001000200030005000 7
      000600046a6a0008dada0009000a044a4acaca02dada0a00010002fe00aaaaff
      000320f47274a5ca029cbaddd6200c6edffe6953673a6dfe14a374dfb2ddb48b
      2805d4044a4a019b404096888fa26228966af730b8e61e9d0f18f9132fff6783
      eabccf7169d3170ceff0d9ad3834ca52802420d1bc68313908cdc1665f82fd3b
      8254b86721f0e7a38606010220ddeb878addd0fae32eedf8b875de7523399bee
      24174453f9e478cab2b5ce7e6b205773519a12267e6ed5c31d4e153a38ccf095
      696d9a871ee1b66d3fe3a23395aa00010220462680fd79ee53114f3f501e2ca4
      102172097b125cbfa8b399e89869d4a5893900004042206fe0ff831a2869776d
      762948f50febdb765cf8c09d3021414729b1779625edd020dfb7450d78d3ca90
      16f4640e6e5f36ce54cc10e8b407a53d8a1016e50093d9b30000000200000004
      411901012037c89d463611a307df9e98b2df32daf0a4aa0a32dca0f590b75c95
      34372f521f20e349c4ab357225bb6fdf57e5d2b53aac7a7afcf0096036ea16e7
      a0f6208265cd0001206b47045927b857930c3fffe23059f96d1111bb84d3fb53
      13094eccfb62e8522a0200011c0001000200030005caca00077a7a00063a3a00
      040008dada0009000a04baba0a0a025a5a0aaaaa00010002fe00ff0001000000
      0000000000ffffffffffffffff050a0a0206334040f513ed0efdbf49964e5ada
      1b63e5b61c5d33e43156ace19d8979e4a95c748ffd328cc8a096d921b4317b9b
      d3282b996a9b0272f5194e8f7dc7b151de5101d30800010220462680fd79ee53
      114f3f501e2ca4102172097b125cbfa8b399e89869d4a589390000404220caf0
      09ad02a57a48feb8d64d055509e9a81edba8d325e442cfe75e006a5200062046
      7a05e466a111ccb79268d040b373aa74442324b021689292d7253ca371faf8
    application_messages:
      -
        00010002202af8e1a35853f84a78f3c49ea2656f505ae35132fd240fedd61a7b
        6084ea16e2000000000000000501001c183146fe9ac9fadd10c1e70076ab8d72
        e78ba6afef5a496de407f1694073282ff405f3b430d71036e08dda902495d3cc
        f53d79fcc7c3ceb83be4906d113d7f89b0695a5f288433e4cc779a7e02d4a703
        47804a992f5c99f8ad0b165d94a956f90cd078fb4bb0a171564df95851c92225
        90cf54b37a0e867b82dad8a9db2a9072efcc84fe334fb0e56fdc291eba8141ff
        67000000010000000441620101 20b8ee593dbb1112f974c4cbb4978440123612
```

```
          2102feb656b5e1df364810e1071f20d02d3c2f629e10e39aeb304a38af3a4d83
          029591345bf72aa53fa6b2dec1a8ab000120764f19155935995dc0e06a8df057
          049b871d094555320a35e7797dfdec200c790200011e000100020003000500070
          000600047a7adada00085a5a2a2a0009000acaca04caca0a0a02dada0a2a2a00
          010002fe00ff000100000000000000000ffffffffffffffff08caca05f1d19dd7
          ce4040c8a448335607f0521196510afb549aaf9e3e7cf07810f0dd854159fe23
          84983a28a629948aec5e42b1d164ff6d1bd94dd5a98477c0a4e8f79288323693
          77120a010220ddeb878addd0fae32eedf8b875de7523399bee24174453f9e478
          cab2b5ce7e6b205773519a12267e6ed5c31d4e153a38ccf095696d9a871ee1b6
          6d3fe3a23395aa00010220462680fd79ee53114f3f501e2ca4102172097b125c
          bfa8b399e89869d4a5893900004042202d1271947cec646a5f0c0eb9a08c1e84
          028a34caaa1bf84a08cbff3dab08cc0c20dfb7450d78d3ca9016f4640e6e5f36
          ce54cc10e8b407a53d8a1016e50093d9b3
      epoch_authenticator:
        13a670728f17ea7543f95756c74d6d4897263ccdf90f565eb9183294509041b7
      proposals: []
```

Appendix B. Known Issues

* To realize the completely optimized performance profile discussed on Section 12, we should define a version of AnnotatedCommit that sends a SplitCommit instead of a normal Commit.

* There is no signaling within the group of whether any members are partial clients, and if so which ones. This was omitted because it didn't seem clearly necessary, but it could be useful. For example, if a client could include a LeafNode extension that declares that it is a partial client, then a committer could use this signal to proactively generate AnnotatedCommits for the members. An approach like this might be necessary if we wanted to enable cases where annotations were confidential to the group.

* There are no WireFormat values registered for the new messages defined here that are likely to be sent on the wire: AnnotatedCommit, AnnotatedWelcome, or SenderAuthenticatedMessage<PrivateMessage>. It's not clear that these WireFormat values would be needed or useful, though, since the annotations added in these messages are effectively outside the bounds of MLS. They're more like how the delivery of the ratchet tree is unspecified in RFC MLS.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Franziskus Kiefer
Cryspen
Email: franziskuskiefer@gmail.com

Karthikeyan Bhargavan
Cryspen
Email: karthik.bhargavan@gmail.com

Richard L. Barnes
Cisco
Email: rlb@ipv.sx

Jol Alwen
AWS Wickr
Email: alwenjo@amazon.com

Marta Mularczyk
AWS Wickr
Email: mulmarta@amazon.ch