```
+---------------------------------------------------------------------+
| IEEE 802.1 REVISION REQUEST 0136                                    |
+------------------===================================----------------+
```

DATE: 8 MAY 2014
NAME: MICK SEAMAN
COMPANY/AFFILIATION: MICK SEAMAN, 802.1 SECURITY TG CHAIR
E-MAIL: mick_seaman@ieee.org

REQUESTED REVISION:
STANDARD: 802.1X
CLAUSE NUMBER: 6.2.1
CLAUSE TITLE: Key derivation function

RATIONALE FOR REVISION:

Since 802.1X-2010 was approved a suitable KDF has been standardized as RFC 5869 (HKDF). This has been brought to our attention in a sponsor ballot comment. The comment's remedy of substituting this for the currently specified AES-CMAC based KDF was out-of-scope and would require more extensive change than first suggested. This maintenance item is intended to record the suggestion for more extensive analysis. Entering this maintenance item is not a suggestion that the change would or should be made, only that it should receive consideration. Such a change would not result in a large implementation change, but might result in a lack of interoperability.

PROPOSED REVISION TEXT:

Add or substitute the RFC 5868 (HKDF) for the current KDF.

IMPACT ON EXISTING NETWORKS:

Potential lack of interoperability with existing implementations. Possible interoperability if both KDFs implemented though that might call into question any security gain. New parameter set identifier would (probably) have to be added to identify uses of the new KDF. A new CKN formulation would be required to identify use of the new KDF in generating a different CAK. Security gain from changing the KDF is not known at present.

```
 +--------------------------------------------------------------------+
| Please attach supporting material, if any                           |
| Submit to:- Tony Jeffree, Chair IEEE 802.1                          |
|  and copy:- Glenn Parsons, Vice-Chair IEEE 802.1                    |
|    E-Mail: stds-802-1-maint-req@ieee.org                            |
|                                                                     |
|            +------- For official 802.1 use -----------+             |
|            | REV REQ NUMBER: 136                       |             |
|            | DATE RECEIVED: May 8 2014                 |             |
|            | EDITORIAL/TECHNICAL                       |             |
|            | ACCEPTED/DENIED                           |             |
|            | BALLOT REQ'D YES/NO                       |             |
|            | Status: R                                 |             |
|            +------------------------------------------+             |
+---------------------------------------------------------------------+
```