# 21-13-0088-00-MuGM

|  |  |  |
| --- | --- | --- |
| GKB\_INDEX | SEQUENCE( NODE\_BIT\_LENGTH, NODE\_INDEX) | This is the base data type for COMPLETE\_SUBTREE. |
| NODE\_BIT\_LENGTH | UNSIGNED\_INT(1) | This stores the bit length of the following NODE\_INDEX. |
| NODE\_INDEX | CHOICE ( UNSIGNED\_INT(1), UNSIGNED\_INT(2), UNSIGNED\_INT(3), UNSIGNED\_INT(4) ) | This stores the index of a node of the binary tree. See 9.4.2.1 for the details. |
| COMPLETE\_SUBTREE | LIST (GKB\_INDEX) | The data type for the complete subtree part of a GKB. See 9.4.2.1 for the details. |
| GROUP\_KEY\_DATA | LIST (ENCRYPTED\_GROUP\_KEY) | The data type for the key data part of a GKB. See 9.4.2.1 for the details. |
| ENCRYPTED\_GROUP\_KEY | OCTET(16) | This is the base data type for GROUP\_KEY\_DATA. This stores a group key of 16 octets encrypted with an AES key of 16 octets. |
| VERIFY\_GROUP\_KEY | SEQUENCE ( OCTETS(16), OCTETS(16)) | The first octets are arbitrary message. The second octets are the MAC value to be verified. |

The data type of VerifyGroupKey is VERIFY\_GROUP\_KEY:

VERIFY\_GROUP\_KEY = SEQUENCE ( OCTET(16), OCTET(16) )

The first OCTET(16) is arbitrary data, which is an input message to AES-CMAC (defined in RFC-4493). The second OCTET(16) is the MAC value for the first OCTET(16) to be verified.