

# Status: Verified (2)

## RFC 2286, "Test Cases for HMAC-RIPEDMD160 and HMAC-RIPEDMD128", February 1998

Source of RFC: Legacy

Errata ID: 463

**Status: Verified**

**Type: Technical**

Reported By: Kevin Springle

Date Reported: 2002-09-17

In the Appendix:

```
/* The HMAC_SHA1 transform looks like:
```

◀

▶

It should say:

```
/* The HMAC_RMD160 transform looks like:
```

◀

▶

---

Errata ID: 627

**Status: Verified**

**Type: Technical**

Reported By: Kevin Springle

Date Reported: 2002-09-17

In the Appendix:

```
/* if key is longer than 64 bytes reset it to key=SHA1(key) */
```

◀

▶

It should say:

```
/* if key is longer than 64 bytes reset it to key=RMD160(key) */
```

◀

▶

Notes: