

## STANDARDS AUSTRALIA

**Amendment No. 1**  
**to**  
**AS 2805.6.2—2002**  
**Electronic funds transfer—Requirements for interfaces**  
**Part 6.2: Key management—Transaction keys**

## REVISED TEXT

The 2002 edition of AS 2805.6.2 is amended as follows; the amendment(s) should be inserted in the appropriate place(s).

SUMMARY: This Amendment applies to Clause 6.4.1 and 6.4.2.

Published on 15 February 2006.

---

**Page 15 Clause 6.4.1**

*Delete* the text of Clause 6.4.1 and *replace* with:

MAC generation is specified in AS 2805, Parts 4.1 and 4.2. The updating of the current terminal key is dependent on the untransmitted residues of the MAC calculations for the initial request and response messages which form a transaction. MAC residues are never transmitted.

This Standard requires that the MAC generation process provides sufficient data for the MAC and a 64-bit MAC residue.

In AS 2805.4.1, the MAC is the leftmost part of, or all of, a 64-bit field called the MAB. In order to obtain sufficient additional data for the MAC residue, a 128-bit Extended MAB shall be formed by concatenating the MAB with a MAB extension. The MAB extension shall be the result of DEA-3-enciphering the MAB using the MAC key. (Refer to Figure 6.1).

In AS 2805.4.2, the MAC is the leftmost part of the hash-code. When used with this Standard, the complete hash-code will be the Extended MAB and the length of the MAC shall be no more than the length of the hash-code minus 64 bits.

---

**Page 15 Clause 6.4.2**

*Delete* the text of Clause 6.4.2 and *replace* with:

MAC residues shall be generated as follows (see Figure 6.2):

- (a) *Request MAC residue* An Extended MAB for the request message is calculated. The leftmost bits of the calculated Extended MAB are appended to the message as the MAC and the 64 bits following the MAC are kept as the MAC residue X.
- (b) *Response MAC residue* The calculation of the Extended MAB for the response message uses the text of the response message preceded by the MAC residue X, and for approved transactions followed by the AP. The construction of the AP is specified in Clause 6.6.7. The MAC residue X and the AP are not transmitted in the response message. The leftmost bits of the calculated Extended MAB are appended to the message as the MAC and the 64 bits following the MAC are kept as the MAC residue Y.

NOTE: The procedure of including the MAC residue from the previous message in the MAC calculation for the current message is known as MAC chaining and is described in Clause 8.5.

AMDT  
No. 1  
FEB  
2006

AMDT  
No. 1  
FEB  
2006

- (c) *Completion messages* If completion messages are transmitted, the calculation of the MAC for each completion message uses the text of the completion message preceded by the MAC residue from the previous message. The leftmost bits of the calculated Extended MAB are appended to the message as the MAC and the 64 bits following the MAC are used for MAC chaining but not for terminal key updating.
-