

STANDARDS AUSTRALIA

Amendment No. 1
to
AS 2805.9—2000
Electronic funds transfer—Requirements for interfaces
Part 9: Privacy of communication

REVISED TEXT

The 2000 edition of AS 2805.9 is amended as follows; the amendments should be inserted in the appropriate places.

SUMMARY: This Amendment applies to Clauses 5.3.2 and 6.3.1, and Appendix B.

Published on 17 June 2011.

AMDT
No. 1
JUN
2011

Clause 5.3.2

- 1 *Add* the following new item *after* list item (vii):
(viii) System Trace Audit Number (Bit map P 11).
- 2 *Add* the following new item *after* list item (G):
(H) System Trace Audit Number (Bit map P 11).

AMDT
No. 1
JUN
2011

Clause 6.3.1

Delete existing text and *replace* with the following:

If transaction keys are not used then the privacy key should be changed for each message in an output feedback mode of operation to prevent unauthorized interception. Example schemes are illustrated in Appendix B.

AMDT
No. 1
JUN
2011

Appendix B

Add the following new text *after* the existing text:

Alternatively, provided it can be assured that the STAN will remain unique during the life of the session key, the SV could be changed for each message in an output feedback mode of operation by XORing it with the STAN as follows:

(SV)=XOR(STAN,X'0123456789ABCDEF')

Where the STAN is right justified and left zero filled for XOR operation.

This page has been left intentionally blank.