

STANDARDS AUSTRALIA

Amendment No. 1
to
AS 2805.6.3—2000
Electronic funds transfer—Requirements for interfaces
Part 6.3: Key management—Session keys—Node to node

REVISED TEXT

The 2000 edition of AS 2805.6.3 is amended as follows; the amendment should be inserted in the appropriate place.

SUMMARY: This Amendment applies to Clause 6.1.2.

Published on 3 March 2003.

AMDT
No. 1
MAR
2003

Page 10, Clause 6.1.2

Delete Clause 6.1.2 and *substitute* the following:

6.1.2 Input

The inputs shall be the DEA 3 KEK, which is a 128-bit value and a constant and shall take one of the following values:

<i>Key to be enciphered by KEK_{Vn}</i>	<i>Value of constant</i>
MAC key (KMAC)	X'24C024C024C024C024C024C024C024C0'
PIN encipherment key (KPE)	X'28C028C028C028C028C028C028C028C0'
Data key (KD)	X'22C022C022C022C022C022C022C022C0'
Random number (RN)	X'82828282828282828282828282828282'
Inverted random number (~RN)	X'84848484848484848484848484848484'

This page has been left intentionally blank.