KEY MANAGEMENT VALIDATION SYSTEM NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

KEY MANAGEMENT VALIDATION SYSTEM (KMVS)

SUCCESSFUL VALIDATIONS
(as of January 22, 1992)

1. LITRONICS Information Systems

2950 Redhill Avenue
Costa Mesa, CA 92626
(Originally validated by Codercard; rights transferred on September 11, 1990)

Bob Gray, (714) 545-6649
James Prohaska, (703) 960-8068
COMPONENTS:

Hardware: Argus-PC, Model: CMS-100 Software: Argus/MACE Software, Version: 1.0 Date of Validation: Sept. 23, 1988 TESTING OPTIONS:

Number of communicating pairs: 2
Number of manual (*)KKs per comm. pair: 2
Length of manual and auto. (*)KKs: PAIR
Key generation capability: YES
Number of auto. distr. (*)KKs shared: UP TO 4
Number of KDs shared: UP TO 8
Two KDs in KSMs: SOMETIMES
Send RSI messages: NOT TESTED
Receive RSI messages: NOT TESTED
Notarization of keys in KSMs: ALWAYS
Send odd parity on keys in KSMs: ALWAYS
Send IVs in KSMs: SOMETIMES
Send encrypted IVs in KSMs: ALWAYS
Send EDCs in RSIs and ESMs: ALWAYS
Action if EDC received in RSIs and ESMs: NOT APPLICABLE
Send EDKs in KSMs: SOMETIMES
Action on count error: ADJUST COUNT
Send DSMs: YES
Receive DSMs: YES
IDA in DSM if only one KD can be shared: YES
Role assumed: EITHER A OR B
Automatic error recovery: NOT TESTED
Space & CRLF as field delimiter: NOT TESTED

2. TECHNICAL COMMUNICATIONS CORPORATION

100 Domino Drive
CONCORD, Massachusetts 01742
John Gill, (617) 862-6035
COMPONENTS:

Hardware: CX5000A
Software: Version: 1.0
Date of Validation: May 6, 1991
TESTING OPTIONS:

Number of communicating pairs: 1
Number of manual (*)KKs per comm. pair: 2
Length of manual and auto. (*)KKs: PAIR
Key generation capability: YES
Number of auto. distr. (*)KKs shared: 0
Number of KDs shared: 1
Two KDs in KSMs: NEVER
Send RSI messages: NOT TESTED
Receive RSI messages: NOT TESTED
Notarization of keys in KSMs: ALWAYS
Send odd parity on keys in KSMs: ALWAYS
Send IVs in KSMs: SOMETIMES
Send encrypted IVs in KSMs: ALWAYS
Send EDCs in RSIs and ESMs: ALWAYS
Action if EDC received in RSIs and ESMs: NOT APPLICABLE
Send EDKs in KSMs: NEVER
Action on count error: ADJUST COUNT
Send DSMs: YES
Receive DSMs: YES
IDA in DSM if only one KD can be shared: YES
Role assumed: EITHER A OR B
Automatic error recovery: NOT TESTED
Space & CRLF as field delimiter: NOT TESTED

3. TECHNICAL COMMUNICATIONS CORPORATION

100 Domino Drive
CONCORD, Massachusetts 01742
John Gill, (617) 862-6035
COMPONENTS:

Hardware: CX5000
Software: Version: 2.0
Date of Validation: May 15, 1991
TESTING OPTIONS:

Number of communicating pairs: 1
Number of manual (*)KKs per comm. pair: 2
Length of manual and auto. (*)KKs: PAIR
Key generation capability: YES
Number of auto. distr. (*)KKs shared: 4
Number of KDs shared: 1
Two KDs in KSMs: NEVER
Send RSI messages: NOT TESTED
Receive RSI messages: NOT TESTED
Notarization of keys in KSMs: ALWAYS
Send odd parity on keys in KSMs: ALWAYS
Send IVs in KSMs: SOMETIMES
Send encrypted IVs in KSMs: ALWAYS
Send EDCs in RSIs and ESMs: ALWAYS
Action if EDC received in RSIs and ESMs: NOT APPLICABLE
Send EDKs in KSMs: NEVER
Action on count error: ADJUST COUNT
Send DSMs: YES
Receive DSMs: YES
IDA in DSM if only one KD can be shared: YES

Role assumed: EITHER A OR B
Automatic error recovery: NOT TESTED
Space & CRLF as field delimiter: NOT TESTED

4. COMMUNICATION DEVICES, INC.

1 Forstmann Court
Clifton, NJ 07011
Tadhg Kelly, (201) 772-6997
COMPONENTS:

Hardware: 917CD
Model: 01-10-0700
Software: RSD/E
Version: 7.2
Date of Validation: January 22, 1992
TESTING OPTIONS:

Number of communicating pairs: 1
Number of manual (*)KKs per comm. pair: 1
Length of manual and auto. (*)KKs: PAIR
Key generation capability: NO
Number of auto. distr. (*)KKs shared: 0
Number of KDs shared: 1
Two KDs in KSMs: NEVER
Send RSI messages: NOT TESTED
Receive RSI messages: NOT TESTED
Notarization of keys in KSMs: ALWAYS
Send odd parity on keys in KSMs: ALWAYS
Send IVs in KSMs: SOMETIMES
Send encrypted IVs in KSMs: ALWAYS
Send EDCs in RSIs and ESMs: ALWAYS
Action if EDC received in RSIs and ESMs: NOT APPLICABLE
Send EDKs in KSMs: NEVER
Action on count error: ADJUST COUNT
Send DSMs: YES
Receive DSMs: YES
IDA in DSM if only one KD can be shared: YES
Role assumed: PARTY B
Automatic error recovery: NOT TESTED
Space & CRLF as field delimiter: NOT TESTED