ISO/TR 19038:2005-06 (E)

Banking and related financial services - Triple DEA - Modes of operation - Implementation guidelines

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviations 4

5 Specifications 5

6 TDEA modes of operation 8

Annex A (informative) ASN.1 syntax for TDEA modes of operation 36

Annex B (informative) TDEA modes of operation cryptographic attributes 42

Annex C (informative) Key bundle encryption precautions 45

Bibliography 54