INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

T.36

Amendment 1
(04/99)

SERIES T: TERMINALS FOR TELEMATIC SERVICES

Security capabilities for use with Group 3 facsimile terminals

Amendment 1

ITU-T Recommendation T.36 – Amendment 1

(Previously CCITT Recommendation)

ITU-T T-SERIES RECOMMENDATIONS

TERMINALS FOR TELEMATIC SERVICES

For further details, please refer to ITU-T List of Recommendations.

ITU-T RECOMMENDATION T.36

SECURITY CAPABILITIES FOR USE WITH GROUP 3 FACSIMILE TERMINALS

AMENDMENT 1

Summary

Amendment 1 to Recommendation T.36 defines the override mode associated with the HKM/HFX encryption system.

Source

Amendment 1 to ITU-T Recommendation T.36 was prepared by ITU-T Study Group 8 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 1st of April 1999.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation the term *recognized operating agency (ROA)* includes any individual, company, corporation or governmental organization that operates a public correspondence service. The terms *Administration, ROA* and *public correspondence* are defined in the *Constitution of the ITU (Geneva, 1992)*.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

1) Subclause A.2.2 1

2) New subclause C.7 1

C.7 Override mode 1

SECURITY CAPABILITIES FOR USE WITH GROUP 3 FACSIMILE TERMINALS

AMENDMENT 1

(Geneva, 1999)

1) Subclause A.2.2

Amend A.2.2 to read as follows:

A.2.2 Functions

Key management is provided using the HKM system defined in Annex C/T.36. Three procedures are defined:

1) the registration mode (see C.4);

2) the secure mode (see C.5); and

3) the override mode (see C.7).

Registration establishes mutual secrets and enables all subsequent transmissions to be provided securely. In subsequent transmissions, the HKM system provides mutual authentication, a secret session key for document confidentiality and integrity, confirmation of receipt and a confirmation or denial of document integrity.

Document confidentiality is provided using the carrier cipher defined in Annex D/T.36. The carrier cipher uses a 12-decimal digit key which is approximately equivalent to 40 bits.

Document integrity is provided using the system defined in Annex E/T.36. This annex defines the hashing algorithm including the associated calculations and information exchange.

2) New subclause C.7

Add a new subclause C.7 to read as follows:

C.7 Override mode

The override mode allows the terminal operators to communicate independently and in secret using two secure facsimile terminals conforming to Recommendation T.36 without carrying out a registration process between the two terminals. This is accomplished by by-passing the automatic key management procedures of the secure mode (see C.5). No mutual primitive is generated, no registered crypt number is retrieved and no secret session key is established. Instead, a mutually agreed pre-arranged 12-digit secret session key is entered by the terminal user at the sending terminal which is used with a carrier cipher to provide document confidentially. The terminal user at the receiving terminal enters the same mutually agreed key which is used with the carrier cipher to decrypt the received document.

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	**Terminals for telematic services**
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure
Series Z	Languages and general software aspects for telecommunication systems