PRIVACY/DATA PRODUCTS INTERFACE

FEATURE DOCUMENT

1A *ESS*™ SWITCH

AUTOPLEX™ SYSTEM 100

CONTENTS PAGE

1. INTRODUCTION

DEFINITION

1.01 The privacy/data products provide both cellular and land customers with high quality private-voice and data services. Private-voice service uses the DES (Data Encryption Standard) algorithm to encrypt voice signals. Data service supports data speeds of 300, 1200, and 2400 bits per second in asynchronous format and also uses the DES algorithm to protect the privacy of data communications. The products may also be used in the clear voice mode.

1.02 Data service provides an automatic answer capability that allows data to be sent to an unattended or moving vehicle.

1.03 Data integrity is protected by a selective repeat or ARQ (automatic repeat request) protocol during handoffs, blank and burst messages, fading, etc. Transmitted data is buffered while a cyclic redundancy check scheme detects errors and requests retransmission, if required.

AVAILABILITY

1.04 This feature is not generic program dependent.

ASSIGNMENT

1.05 The Privacy/Data Products Interface feature is available on a per MTSO (mobile telephone switching office) basis.

1.06 Cellular system providers may offer mobile customers privacy/data service for the radio segment of all calls on a subscription basis. A separate DN (directory number) is required.

1.07 Customers may make private-voice/data service calls between CTS 1620 privacy/data accessories without involving the switching office feature.

INTERACTIONS

1.08 Customers involved in a private-voice/data service call should consider the following features:

(a) ***Three-Way Calling:*** A customer involved in a private-voice/data service call should not add on a third party.

(b) ***Call Waiting:*** While not prohibited, subscribers should be advised not to also subscribe to the Call Waiting feature. Call waiting tones can produce audible noise during private-voice service calls. During data service calls, call waiting tones interrupt carrier resulting in a loss of data.

Note: Both of these features operate normally in the clear-voice mode.

1.09 Roamer II service uses a temporary local DN for roaming that allows customers to subscribe to private-voice/data service in a foreign area.

2. PRODUCT DESCRIPTION

2.01 The product line consists of the following types of equipment:

- CTS 1620 Privacy/Data Accessory (1AMAS)
- SRE (Switch Resident Equipment) consisting of SCUs (SRE Channel Units) and associated equipment.

The CTS 1620s and SCUs communicate in pairs, like data sets, over a voiceband transmission path using a proprietary protocol. All units can provide both private-voice and data service.

2.02 The product line also consists of two modules, an FKM (fixed key module) and a CKM (configuration and key module).

MOBILE RESIDENT UNIT

2.03 The CTS 1620 resides in the cellular customer's vehicle, either in the trunk or in the passenger compartment. It is connected to the cellular telephone at the interface between the control unit and the transceiver unit. For data service, DTE (data terminal equipment) is connected to the CTS 1620 via an EIA (Electronic Industries Association) RS-232C cable.

KEY MODULES

2.04 Encryption keys are required to start private-voice and data service calls. Each CTS 1620 can store up to 64 encryption key records in an EEROM (electrically eraseable read only memory) which retains data when power is off. Each encryption key record consists of a master key and a KIN (key identification number).

2.05 At the beginning of a private-voice or data call, the units exchange KINs and determine which, if any, prestored encryption key to use. If the CTS 1620 does not have a common prestored encryption key, they use the default encryption key known to all units. Although this results in reduced security, the channel is nevertheless protected from casual listening by a third party.

A. Configuration and Key Module

2.06 A CKM is supplied with each CTS 1620. It consists of a mode switch, 16 configuration switches, and an EEROM chip containing one encryption key record. It has two modes, as follows, controlled by the mode switch.

(a) The configuration mode is used to feed the default configuration selections into the CTS 1620.

(b) The key mode is used to assign (write) a random encryption key record into the CKM, then feed it into other CTS 1620s for end-to-end calls.

2.07 The KIN in a CKM consists of a 1 in the first bit followed by 31 random bits.

B. Fixed Key Module

2.08 An FKM is used for service provided by cellular system providers for the CTS 1620-to-SCU

portion of the call and not for end-to-end calls. The FKM contains a PROM (programmable read only memory) chip containing one encryption key record. This record is programmed at the factory and cannot be changed by customers.

2.09 Mobile subscribers use FKMs to feed encryption key records to their CTS 1620s.

2.10 A 10-digit KIN is printed on the surface of the FKM and its sealed shipping container. Mobile subscribers and cellular service providers do not normally know the content of FKM encryption keys.

2.11 The FKM KIN consists of a 0 first digit, a 12-bit system index, and a 19-bit master key index. The system index is associated with a specific cellular system. It is assigned by the FKM supplier and is different from the cellular SID (system identification). The master key index specifies the address location of a master key in SRE key processors.

SWITCH RESIDENT EQUIPMENT

2.12 The SRE consists of the following equipment:

- Common control processor having two operations processors and two key processors
- A variable number of SCUs and data sets.

Duplicated operations and key processors provide high reliability.

A. SRE Operations Processors

2.13 The SRE operations processors consist of terminals, processors, and optional disk drives. They provide the following functions:

(a) ***Security Dial Back:*** This capability allows remote access to the processors.

(b) ***Equipment Test:*** Upon request, processors perform operational tests on the SCUs and report results.

(c) ***SCU Software Down Load:*** The processors can down load software to each SCU for the purposes of rebooting, changing software, or updating the generic program.

(d) ***Record Keeping:*** The SRE operations processors keep the following records.

(1) ***Class of Service:*** The class of service record for each KIN indicates: private-voice service, data service, combined private-voice and data service, or no service. The SRE limits service to that indicated by the service record. The records are changeable by cellular system providers.

(2) ***Data Collection:*** Monitors SCU usage and produces records detailing privacy/data call histories.

B. SRE Key Processors

2.14 The SRE key processors provide encryption key records to all SCUs. Each processor has a ROM (read only memory) circuit pack containing up to one-half million prerecorded encryption words. At the beginning of each private-voice or data service call, the key processor uses the KIN (received from the CTS 1620) to retrieve the proper encryption key.

C. SRE Channel Unit

2.15 The SCU is connected in the MTSO to either network interface trunks or loop-around trunks. It is compatible with 4-wire E&M type II trunks. The SCUs respond to request (signaling tones) from CTS 1620s for private-voice and data services.

2.16 For data service, SCUs provide modem functions that are compatible with 212AR and 2224 data sets, thus enabling CTS 1620s to communicate with computer modems.

2.17 Mobile-to-mobile private-voice and data service calls are provided by installing two SCUs back to back on loop-around trunks. This arrangement allows the individual CTS 1620s to use different encryption keys.

2.18 The SCUs are mounted in a channel unit cabinet (J-41657B) which is supplied with a minimum configuration of 16 units. The SCUs can be grown in increments of 8 units (channels) for a maximum of 48 channels per cabinet.

2.19 When a second channel cabinet is added, a common control cabinet (J-41657A) must also

be provided. This cabinet can control up to 12 channel cabinets. (This 576-channel maximum configuration can accommodate approximately 14,000 subscribers.)

D. Data Sets

2.20 One 2224 data set (modem) is required in the MTSO for each SCU. When signaling tones from the CTS 1620 indicate a request for data service, the SCU connects the data set. The data sets are housed in a modem cabinet (J-41657C) which has a minimum configuration of 16 data sets. Growth is in increments of 8; the cabinet has a maximum capacity of 96 data sets.

E. Trunking Modifications

2.21 A 4-wire path has been provided between the CTS 1620 and SCU. This 4-wire path eliminates the need for echo cancelers and the resulting 2-second gap following handoff. Since the physical path through the 1A ESS switch is 2-wire, equivalent 4-wire is accomplished by frequency multiplexing the regular voiceband with a 20-kHz frequency band. A 20-kHz modulator circuit is contained in each SRU and a 20-kHz demodulator circuit is added to each SD-1A236-05 cell-site trunk circuit.

2.22 Voice signals toward a mobile customer use the 20-kHz frequency band; voice signals from a mobile customer use the baseband. Zone-office trunks and loop-around trunks are not equipped with demodulators.

3. USER PERSPECTIVE

SERVICE PROVISION

3.01 To obtain private-voice and data services, customers need to purchase or lease CTS 1620s and FKMs from cellular service providers, their resale agents, or other retailers. There are two distinct types of services: service provided by cellular service providers and end-to-end use. A customer may obtain both types of service.

3.02 The service provided by the cellular service provider allows the mobile user to make/receive private-voice calls. The portion of the call between the mobile user and the MTSO is encrypted.

3.03 End-to-end calls can be made between CTS 1620s without subscribing to the cellular service provider's service. However, encryption does not apply to any other calls.

TYPES OF CALLS

3.04 In the following discussions, mobile customers who subscribe to the private-voice/data services provided by cellular system providers are called "subscribers". All other customers (mobile or land) are termed "nonsubscribers".

Mobile-to-Land Calls

3.05 ***Private-Voice Calls From a Subscriber to a Land Customer:*** These calls involve a CTS 1620 and an SCU. Calls are encrypted only over the radio link.

3.06 ***Data Calls From a Subscriber to a Land Customer:*** These calls involve a CTS 1620 and an SCU (including a modem) where the land customer has a data set. Calls are encrypted only over the radio link.

Land-to-Mobile Calls

3.07 ***Private-Voice Calls From a Land Customer to a Subscriber:*** These calls involve a CTS 1620 and an SCU. Calls are encrypted only over the radio link.

3.08 ***Data Calls From a Land Customer to a Subscriber:*** These calls involve a CTS 1620 and an SCU (including a modem) where the land customer has a data set. Calls are encrypted only over the radio link.

Mobile-to-Mobile Calls

3.09 ***Calls Involving Two Subscribers:*** These private-voice and data calls involve two CTS 1620-SCU pairs. Separate encryption keys are used.

3.10 ***Calls Involving One Subscriber:*** If the nonsubscriber has a CTS 1620, one CTS 1620-SCU pair is involved. The default encryption key is used for the nonsubscriber segment. If the nonsubscriber has no CTS 1620, privacy is protected only over the subscriber CTS 1620-SCU segment of the call.

3.11 ***Calls Involving Nonsubscribers:*** These end-to-end private-voice and data calls involve a pair of CTS 1620s. No SCUs are involved.

USER OPERATION

3.12 For user operations required to use the CTS 1620s, refer to the CTS 1620 Privacy/Data Accessory User's Manual.

4. CELLULAR SYSTEM PROVIDERS

MTSO ENGINEERING

4.01 Routing of private-voice and data service calls is accomplished by using a special group of cellular DNs and defining the proper rate-center routing in the MTSO.

4.02 System providers need to coordinate the establishment of SCU-equipped trunk group(s) and associated translation data with the zone office(s) for proper routing of all incoming private-voice and data service calls to mobile subscribers. Trunk group traffic measurements, collected at the MTSO, and long-term forecasts should be used to size and reconfigure the SCU-equipped trunk groups.

ADMINISTRATIVE FUNCTIONS

4.03 Cellular system providers should update and maintain each subscriber's class-of-service record.

4.04 The ROM circuit packs in the SRE key processors should be periodically replaced with new ones. Encryption key usage records should be provided to the supplier who can determine which KINs should be changed. The supplier should maintain the uniqueness of the FKM encryption key records and administer the encryption keys in the ROM circuit packs.

MAINTENANCE

4.05 The SCUs provide status indicators that identify failed units. When a SCU has an internal failure, it disconnects the E&M leads and applies an off-hook signal to both the MTSO and network interface end. This causes the MTSO to report the trouble automatically and prevents the zone office from seizing the trunk. When a trunk failure is indicated, cellular system providers should check the SCU status indicators before diagnosing the trunk.

4.06 A 20-kHz modulator circuit has been added to the ROTL (remote office test line) to enable it to be used to test the demodulators in the cell-site trunks. When the ROTL tests a cell-site trunk, it places the modulator in series with the demodulator of the cell-site trunk. The modulator-demodulator operation appears transparent to the ROTL tests, if operating properly.

4.07 The modulator is located in the 52A responder. The ROTL program turns it on at the beginning of a cell-site trunk test and turns it off at the beginning of a zone-office or loop-around trunk test. This is accomplished using signal distributors or central pulse distributors.

5. SUPPLEMENTARY INFORMATION

ABBREVIATIONS

5.01 The following abbreviations are used in this practice:

CKM—Configuration and Key Module

DES—Data Encryption Standard

DTE—Data Terminal Equipment

EEROM—Electrically Eraseable Read Only Memory

EIA—Electronic Industries Association

FKM—Fixed Key Module

KIN—Key Identification Number

LRU—Land Resident Unit

MRU—Mobile Resident Unit

MTSO—Mobile Telephone Switching Office

PROM—Programmable Read Only Memory

ROM—Read Only Memory

SCU—SRE Channel Unit

SID—System Identification

SRE—Switch Resident Equipment.

REFERENCES

5.02 The following documents are applicable to this feature:

(1) CTS 1620 Privacy/Data Accessory User's Manual

(2) AT&T 231-200-005—Mobile Telephone Switching Office, Cell Site, and Subscriber's Unit—System Description

(3) AT&T 231-090-219—Remote Office Test Line—Feature Document

(4) AT&T 231-218-301—Recent Change Formats and Implementation—Description and Procedures

(5) AT&T 231-290-609—Three-Way Calling—Feature Document

(6) AT&T 231-290-610—Call Waiting—Feature Document

(7) AT&T 231-290-616—Roamer II—Feature Document

(8) AT&T 231-390-212—Cellular Mobile Radio Office—Feature Document.

6. COMMENT FORM

6.01 A comment form is located at the back of this practice to provide a communications channel from the user to the writer.

COMMENT FORM

Your comments and suggestions concerning accuracy, level of coverage, organization, etc., of this document will be appreciated. Please be as specific as possible for technical comments.

( ) Check to request reply (technical comments only, please).

Mail comments to:

AT&T Consumer Products
Dept. COWR251350
2400 Reynolda Road
Winston-Salem, N.C. 27106

AT&T Practice _____

Name _____ Tel (___) _____

Co. _____

Address _____

City, State _____ Zip _____