GA

PUBLIC SECURITY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 33.060.01

A 90

GA/T 1059-2013

Police Digital Trunking Communication System - Security Technical Specifications

警用数字集群（PDT）通信系统安全技术规范

Issued on: March 20, 2013 **Implemented on: March 20, 2013**

Issued by: Ministry of Public Security of the People's Republic of China

Table of Contents

Police Digital Trunking Communication System - Security Technical Specifications

1 Scope

This Standard specifies the technical specifications and requirements for authentication, air interface security and end to end security applied in the police digital trunking (PDT) communication system.

This Standard is applicable to the construction and application of the security encryption subsystem of the police digital trunking (PDT) communication system.

2 Normative References

The following documents are indispensable to the application of this document. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GA/T 1056-2013 Police Digital Trunking Communication System - General Technical Specifications

GA/T 1057-2013 Police Digital Trunking Communication System - Technical Specifications for Physical Layer and Data Link Layer of Air Interface

GA/T 1058-2013 Police Digital Trunking Communication System - Technical Specifications for Call Control Layer of Air Interface

3 Terms, Definitions and Abbreviations

3.1 Terms and Definitions

The terms and definitions defined in GA/T 1056-2013, GA/T 1057-2013 and GA/T 1058-2013, and the following are applicable to this document.

3.1.1 authentication

The process of verifying the legitimacy of the identities of communication participants.

3.1.2 stun

The process of temporarily disabling a mobile station using air interface signaling.

3.1.3 revive

The process of unlocking a mobile station that has been stunned using air interface signaling.

3.1.4 kill

The process of permanently disabling a mobile station using air interface signaling. A killed mobile station cannot be unlocked through air interface signaling.

3.1.5 authentication center

A security entity responsible for authenticating with mobile stations.

3.1.6 authentication key

A key used during authentication.

3.1.7 random challenge

The random number generated when the authentication center authenticates with a mobile station.

3.1.8 sequence number

During authentication, the information between the authentication center and the mobile station used to prevent replay attacks.

3.1.9 stun / kill / revive token

A security confirmation code when the trunked station performs stun / kill / revive operations on the mobile station.

3.1.10 synchronization random challenge

The random number generated when the authentication center and the mobile station perform authentication sequence number synchronization operations.

3.1.11 synchronization token

A security confirmation code when the mobile station synchronizes the authentication sequence number with the authentication center.

3.1.12 authentication cryptographic algorithm

The cryptographic algorithm used by the authentication center and the mobile station during authentication.

3.1.13 air interface security

The security mechanism that protects information transmitted on the wireless channel between

the mobile station and trunked station. It is also known as air security for short and includes air interface encryption and integrity protection.

3.1.14 air interface cipher key

A cipher key used in air interface security, including derived cipher key DCK, broadcast cipher key BCK, common cipher key CCK, group cipher key GCK and static cipher key SCK, etc.

3.1.15 air interface cryptographic algorithms

The cryptographic algorithm used by the base station and mobile station during air interface encryption process.

3.1.16 end to end security

A security mechanism that provides full protection to the information transmitted between the transmitting end and the receiving end, including end to end voice encryption and end to end data security.

3.2 Abbreviations

The abbreviations defined in GA/T 1056-2013, GA/T 1057-2013 and GA/T 1058-2013, and the following are applicable to this document. For ease of use, some abbreviations in GA/T 1056-2013, GA/T 1057-2013 and GA/T 1058-2013 are repeatedly listed here.

AIEAID: Air Interface Encryption Algorithm Identity

AIV: Air Interface Initialization Vector

AuC: Authentication Center

BCK: Broadcast Cipher Key

CACH: Common Announcement Channel

CC: Color Code

CCK: Common Cipher Key

CCKID: Common Cipher Key Identity

CCL: Call Control Layer

CCSUM: Cryptographic Checksum

CHAN: Channel Number

CRC: Cyclic Redundancy Check

CSBK: Control Signaling Block

CSBKO: CSBK Opcode

CSC: Common Slot Counter

DBSN: Data Block Serial Number

DCK: Derived Cipher Key

DLL: Data Link Layer

DMO: Direct Mode

E2EE: End to End Encryption

ECK: Encryption Cipher Key

EMB: Embedded Signaling Field

FEC: Forward Error Correction

FID: Feature set ID

FLC: Full Link Control

FN: Frame Number

GCCK: Group Common Cipher Key

GCK: Group Cipher Key

IV: Initialization Vector

ICF: Integrity Check Factor

KI: Key Index

KSS: Key Stream Segment

LB: Last Block

LC: Link Control

MBC: Multiple Block Control

MFID: Manufacturer's specific FID

MFN: Multiframe Number

MS: Mobile Station

4) Utilize algorithm PA1 to calculate TSAuthCode and TSConfCode;

5) The system sends RAND, SEQ and TSAuthCode to MS.

b) The authentication response process on the MS side:

1) The MS receives RAND, SEQ and TSAuthCode from the system;

2) Compare SEQ with SEQ_{MS} locally stored by the MS:

---If SEQ ≤ SEQ_{MS} or SEQ ≥ SEQ_{MS} + WINSIZE, the MS returns an authentication failure message to the system and ends the authentication operation flow;

---If SEQ_{MS} < SEQ < SEQ_{MS} + WINSIZE, continue the following operation flow;

3) Utilize algorithm PA1 to calculate XTSAuthCode and XTSConfCode;

4) Compare XTSAuthCode with TSAuthCode:

---If they are inconsistent, return the authentication failure message to the system and end the authentication operation flow;

---If they are consistent, continue the following operation flow;

5) Utilize algorithm PA2 to calculate MSAuthCode;

6) The MS sends MSAuthCode to the system;

7) The MS saves the received sequence number SEQ as the new local sequence number SEQ_{MS}.

c) The authentication verification process on the system side:

1) The system receives MSAuthCode from the MS;

2) AuC utilizes algorithm PA2 to calculate XMSAuthCode;

3) Compare XMSAuthCode with the received MSAuthCode:

---If they are inconsistent, the system returns the authentication failure message to the MS and ends the authentication operation flow;

---If they are consistent, the system returns an authentication success message containing TSConfCode to the MS.

d) The confirmation process on the MS side:

1) The MS receives the MS authentication success message containing TSConfCode from the system;

a) Synchronization initiation process on the system side:

1) The AuC generates synchronization random number SyncRAND;

2) The system sends SyncRAND to the MS.

b) Synchronization response process on the MS side:

1) The MS receives SyncRAND;

2) Obtain the locally stored sequence number SEQ_{MS};

3) Utilize algorithm PA5 to calculate SyncToken;

4) The MS sends SEQ_{MS} and SyncToken to the system.

c) Synchronization verification process on the system side:

1) The system receives SEQ_{MS} and SyncToken;

2) The AuC utilizes algorithm PA5 to calculate XSyncToken;

3) Compare XSyncToken with SyncToken:

---If they are inconsistent, the synchronization operation fails;

---If they are consistent, the AuC synchronizes the sequence number SEQ_{AuC} corresponding with the MS to SEQ_{MS}.

5.5 Signaling Operation Flow

5.5.1 Two-way authentication

During the registration, the signaling operation flow of two-way authentication is shown in Figure 5, and the signaling operation flow of two-way authentication initiated by the TS is shown in Figure 6. The flow chart adopts MSC. See the detailed format in Appendix A.

6 Air Interface Security

6.1 Overview

Air interface security protects information transmitted on the wireless channel between the mobile station and the trunked station. Air interface security includes air interface encryption and air interface integrity protection.

6.2 Air Interface Cipher Key

Air interface cipher key is divided into derived cipher key DCK, broadcast cipher key BCK, common cipher key CCK, group cipher key GCK and static cipher key SCK, etc. For BCK and CCK, four different key lengths of 40/64/80/128 bits can be selected based on the security demands. However, the key lengths selected for BCK and CCK shall be consistent; for DCK, GCK and SCK, the key lengths are fixed to 128 bits. The detailed functions of different types of air interface cipher keys are as follows:

a) Derived cipher key DCK

The derived cipher key DCK is generated during the authentication process and is used to manage air interface cipher keys and ensure the security of air interface service data. After each authentication succeeds, a new DCK shall be generated and the old DCK shall be discarded. For different MS, DCK is different.

During the air interface cipher key management process, DCK can be used to protect the common cipher key CCK, broadcast cipher key BCK, group cipher key GCK and static cipher key SCK issued by the system to the MS. DCK can also be used to protect the voice and data bodies in the uplink and downlink directions during single calls, but it shall not be used to protect signaling and data heads.

b) Broadcast cipher key BCK

Broadcast cipher key BCK is generated by the system and is used to protect the common cipher key CCK distributed through broadcast messages. BCK shall be regularly updated in accordance with the security policy, encrypted and protected by DCK, then, distributed to the MS. BCK is shared by a group of MSs under the same TS.

The system assigns a key identification BCKID to each different BCK (the BCKID with a value of 0 is reserved).

The system may decide whether to enable BCK based on actual demands.

c) Common cipher key CCK

D---cipher key stream generation algorithm;

E---vocoder;

F---appropriation;

G---extraction.

Figure 25 -- Schematic Diagram of Synchronization Mechanism

The end to end voice encryption synchronization flow between the sender and the receiver is specifically as follows:

a) Sender flow:

1) In accordance with cipher key index (KI), group call / individual call identification (G/I), TMSI and SMSI, determine the cipher key TEK used for communication;

2) When a voice call starts, a new initialization vector (IV) is generated by a random number generator;

3) Calculate the end to end encrypted control frame cryptographic checksum CCSUM;

4) Construct an end to end encrypted control frame and send it;

5) Utilize the cipher key derivation algorithm to generate the cipher key CK;

6) Generate the voice frame sequence number (FN) from the voice frame counter. Every time a frame of voice is encrypted, the counter automatically increases;

7) Utilize the cipher key stream generation algorithm to calculate the cipher key stream KS;

8) XOR KS with a frame of plaintext voice data to obtain the ciphertext voice data;

9) In the ciphertext voice data, appropriate information bits to carry the FN, form the cipher text voice frame, then, send it.

b) Receiver flow:

1) Obtain G/I, TMSI and SMSI information through signaling GRANT/Grp_V_ch_Usr/UU_V_Ch_Usr, etc.;

2) Extract KI from the received end to end encrypted control frame;

3) In accordance with KI, G/I, TMSI and SMSI, determine the TEK used for communication;

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------