Security Access Algorithm and Code for EMS

1、 This document is used to explain the Security Access Algorithm for the service 0x27 of Changan UDS on CAN diagnosis requirements specification. The Security Access Key received form the tester is calculated from the 4 byte Seed provided by EMS. The 4 byte key is calculated as below.

1) Acquire 4 byte seed from ECU. Say Seed [4].

2) Perform Bitwise Ex-OR operation of seed with a constant, AppKeyConst [4], to obtain Key1 [4].

Key1 [0] = Seed [0] ^ AppKeyConst [0]

Key1 [1] = Seed [1] ^ AppKeyConst [1]

Key1 [2] = Seed [2] ^ AppKeyConst [2]

Key1 [3] = Seed [3] ^ AppKeyConst [3]

3) Rotate the seed [4] by 16 bits to obtain Seed2 [4].

4) Perform Bitwise Ex-OR operation of seed2 with the same constant, AppKeyConst [4], to obtain Key2 [4].

Key2 [0] = Seed2 [0] ^ AppKeyConst [0]

Key2 [1] = Seed2 [1] ^ AppKeyConst [1]

Key2 [2] = Seed2 [2] ^ AppKeyConst [2]

Key2 [3] = Seed2 [3] ^ AppKeyConst [3]

5) Add Key1 and Key2 and discard the final carry bit if any to obtain the key (Key [4]).

2、 The Code, AppKeyConst [4] of EMS is **0x70F27304**.

3、 Calculated examples.

Seed（Hex）	**Seed2（Hex）**	**Key1（Hex）**	**Key2（Hex）**	**Key（Hex）**
12345678	1E6A2C48	62C6257C	6E985F4C	D15E84C8
4711CAFE	7F5388E2	37E3B9FA	0FA1FBE6	4785B5E0
70F27304	20CE4F0E	00000000	503C3C0A	503C3C0A

Examples for seed2 rotated from the seed.

Seed（Hex）	**Seed（Bin）**	**Seed2（Hex）**	**Seed2（Bin）**
12345678	0001 0010 0011 0100 0101 0110 0111 1000	1E6A2C48	0001 1110 0110 1010 0010 1100 0100 1000
4711CAFE	0100 0111 0001 0001 1100 1010 1111 1110	7F5388E2	0111 1111 0101 0011 1000 1000 1110 0010

70F27304	0111 0000 1111 0010 0111 0011 0000 0100	20CE4F0E	0010 0000 1100 1110 0100 1111 0000 1110