SONY®

FeliCa Lite-S

FeliCa Lite-S

Diversified Card Key

Standard Generation Algorithm

Version 1.01

No. M744-E01-01

- FeliCa is a contactless IC card technology developed by Sony Corporation.
- FeliCa is a trademark of Sony Corporation.
- All names of companies and products contained herein are trademarks or registered trademarks of the respective companies.
- No part of this document may be copied, or reproduced in any form, without the prior consent of Sony.
- Information in this document is subject to change without notice.
- Sony assumes no liability for damages arising from, or in connection with, the use of this document.

Introduction

This document describes the standard algorithm for the generation of unique (that is, diversified) card keys for FeliCa Lite-S.

The intended audience of this document is anyone responsible for any of the following:

- setting diversified card keys for FeliCa Lite-S cards (at the time of their issuance)
- performing authentication of cards, using the diversified card keys.

In this document:

- Any product of the FeliCa Lite-S series is expressed as "FeliCa Lite-S".
- FeliCa Lite-S card is expressed as "card".

Unless otherwise specified, the following notational conventions apply in this document:

- Numerical values are expressed in decimal notation.
- By appending "h" to a value, a hexadecimal number is identified.
- By appending "b" to a value, a binary number is identified.
- Unless otherwise specified, the Byte order is Big Endian.

Contents

1 Card key diversification for FeliCa Lite-S

For FeliCa Lite-S, you can set a card key with a size of 16 Bytes. This card key is used in the MAC-generation function. Using the MAC-generation function, the card can be authenticated (that is, the card has the valid key). For details of FeliCa Lite-S, the MAC-generation function of FeliCa Lite-S, and authentication, see the "FeliCa Lite-S User's Manual".

When performing procedures such as authentication using the MAC-generation function of FeliCa Lite-S, you must prevent such card keys from being known to unauthorized people, by keeping the card key secret. A third party that acquires the card key can create duplicate cards that have the same card key.

In the set-up procedure for card keys, set the card keys so that each card has a unique card key. In this document, such a key is referred to as Diversified Card Key.

This document describes the standard algorithm for the generation of Diversified Card Key. When generating that key, it is recommended you use the standard algorithm for that purpose, as described in this document.

2 Standard generation algorithm

This chapter describes the standard algorithm for the generation of Diversified Card Key for FeliCa Lite-S.

2.1 Overview

The standard algorithm generates a Diversified Card Key of 16 Bytes, based on 24 Bytes of data known as Master Key for diversification (in this document, such a key is referred to as Master Key) and the value of the ID block (16 Bytes) set on the card. Using this standard algorithm makes it possible to generate Diversified Card Key, based on the same Master Key and the card-specific values of the ID block.

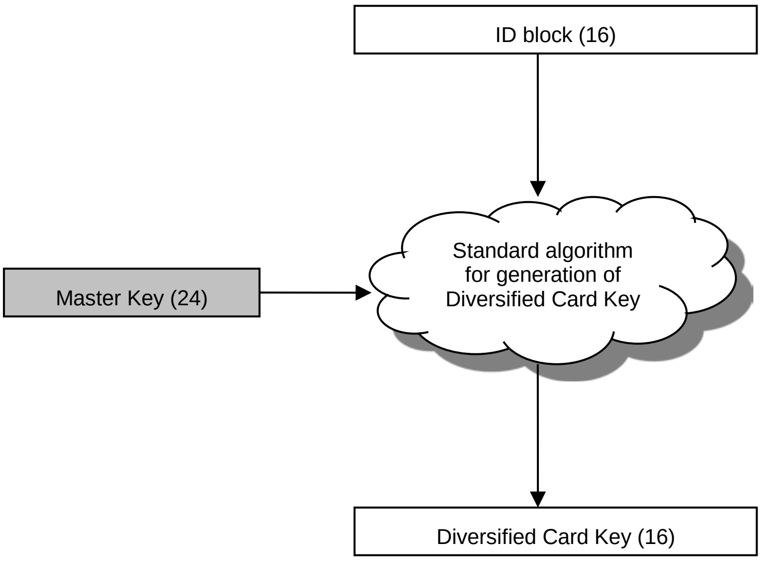
ID block (16)
Master Key (24)
Standard algorithm for generation of Diversified Card Key
Diversified Card Key (16)

Figure 2-1: Diagram of standard algorithm for the generation of Diversified Card Key

When handling Master Key and Diversified Card Key, be especially careful to prevent leakage or loss of these keys. You can use the same value for Master Key if you use that key for the same purpose. In the version management of Master Key, use keys that differ per card key version, which are set to the CKV block.

2.2 Algorithm

The standard algorithm for the generation of Diversified Card Key is as follows:

- Let the value of CMAC (8 Bytes) be T, calculated by 3-key Triple DES (3DES), using Master Key (24 Bytes) as the key and the value of the ID block (16 Bytes) as the message.
- Let the value of CMAC (8 Bytes) be T', calculated by 3-key Triple DES, using the value of ID block (16 Bytes) of which the highest bit is inverted as the message.
- Append T' to T and use the result as Diversified Card Key.

For CMAC, see "NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", published by National Information System for Science and Technology (NIST).

For 3-key Triple DES, see "NIST Special Publication 800-67 Version 1.1, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", published by NIST.

2.3 Procedures

Procedures for the generation of Diversified Card Key using the standard algorithm are as follows:

1) Let Master Key (24 Bytes) be K.

   Let the value (16 Bytes) of ID block be M.

2) Let 0000000000000000h (8 Bytes) be plain text.

   Perform Triple-DES encryption using K as the key and let the result of the encryption be L.

   NOTE The phrase "Perform Triple-DES encryption using K as the key" means perform the following procedure:

   a) Let the Byte strings resulting from the division of K into sectors of 8 Bytes each from the top of K be K_A, K_B and K_C.

   b) Encrypt the plain text using KA as the encryption key.

   c) Decrypt the encrypted data using KB as the decryption key.

   d) Encrypt the result of the decryption using KC as the encryption key.

3) If the highest bit of L is 0, let the result of shifting L to the left by 1 bit be K_1.

   If the highest bit of L is 1, however, let Exclusive-OR of the result of shifting L to the left by 1 bit and 000000000000001Bh (8 Bytes) be K_1.

   NOTE The phrase "shifting L to the left by 1 bit" means to double the value of L and then to discard the highest bit. In addition, Exclusive-OR is calculated on a bit-by-bit basis.

4) Divide M into sectors of 8 Bytes each from the top of M.

   Name the results M_1 and M_2*, respectively.

5) Let Exclusive-OR of M_2* and K_1 on a bit-by-bit basis be M_2.

6) Let M_1 be plain text and let K be the key.

   Perform Triple-DES encryption.

   Let the result of the encryption be C_1.

7) Let Exclusive-OR of C_1 and M_2 be plain text and let K be the encryption key.

   Perform Triple-DES encryption.

   Let the result of the encryption be T.

8) Let the result of the inversion of the highest bit of M_1 (that is, Exclusive-OR with 8000000000000000h) be M'_1.

9) Let M'_1 be plain text and let K be the encryption key.

   Perform Triple-DES encryption and let the result of the encryption be C'_1.

10) Let Exclusive-OR of C'_1 and M_2 be plain text and let K be the encryption key.

    Perform Triple-DES encryption and let the result of the encryption be T'.

11) Append T' to T and let the result be C (16 Bytes), which is Diversified Card Key.

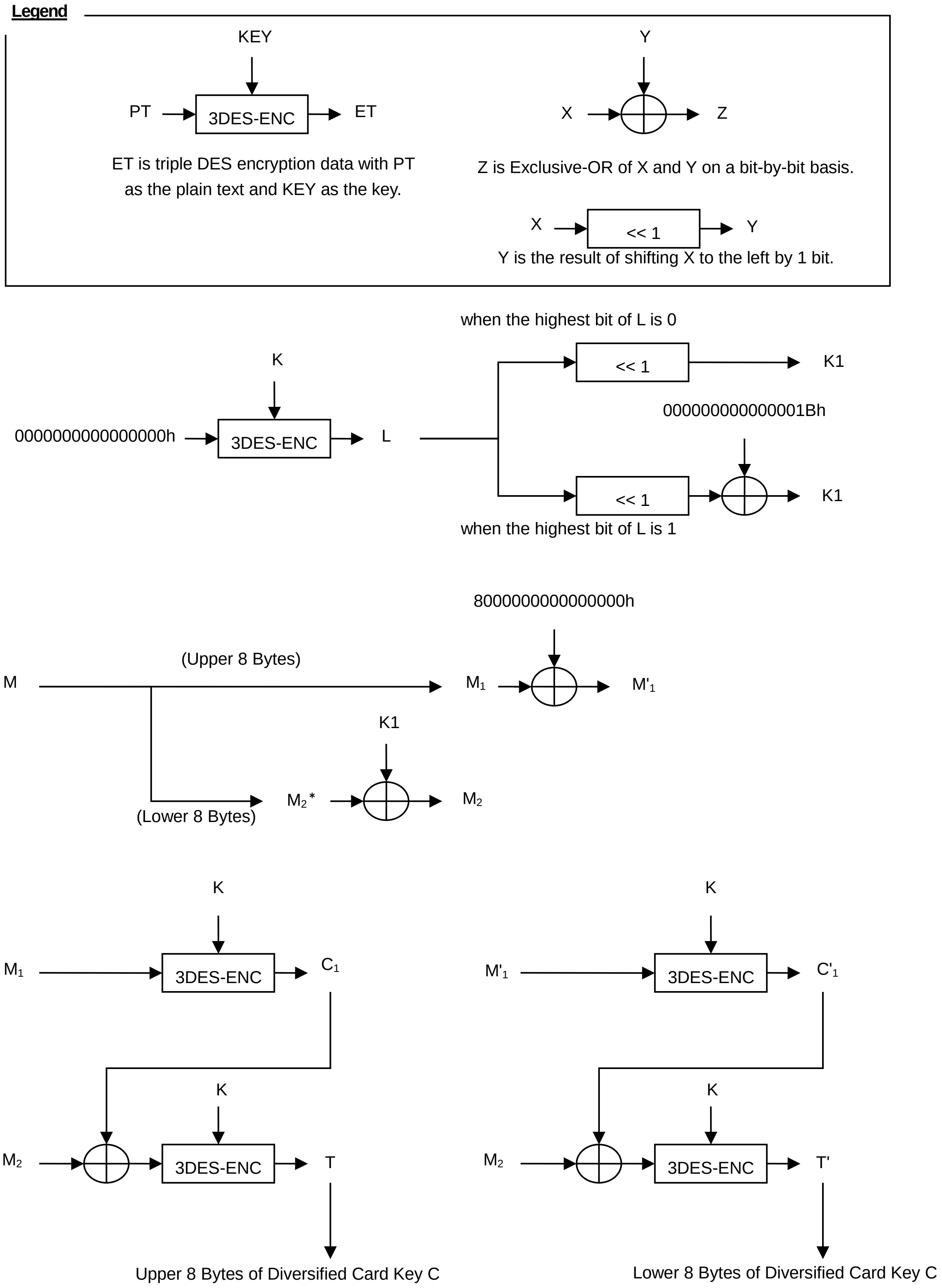
Legend
KEY
PT
3DES-ENC
ET
ET is triple DES encryption data with PT as the plain text and KEY as the key.
Y
X
Z
Z is Exclusive-OR of X and Y on a bit-by-bit basis.
X
<< 1
Y
Y is the result of shifting X to the left by 1 bit.
when the highest bit of L is 0
K
<< 1
K1
0000000000000001Bh
0000000000000000h
3DES-ENC
L
<< 1
K1
when the highest bit of L is 1
8000000000000000h
(Upper 8 Bytes)
M
M1
M'1
K1
M2*
M2
(Lower 8 Bytes)
K
K
M1
3DES-ENC
C1
M'1
3DES-ENC
C'1
K
K
M2
3DES-ENC
T
M2
3DES-ENC
T'
Upper 8 Bytes of Diversified Card Key C
Lower 8 Bytes of Diversified Card Key C

Figure 2-2: Procedure for the generation of Diversified Card Key

FeliCa Lite-S

FeliCa Lite-S Diversified Card Key Standard Generation Algorithm Version 1.01

March 2012	First Edition	FeliCa Business Division
April 2017	Revision	

Sony Imaging Products & Solutions Inc.

No. M744-E01-01

Printed in Japan