SONY®

FeliCa Lite-S

FeliCa Lite-S

Security Application Note

Version 1.11

No. M743-E01-11

- 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 contains important notes about the security functionality provided by FeliCa Lite-S when performing a Service with FeliCa Lite-S.

You are advised to read this document if you develop (or are planning to develop) applications for FeliCa Lite-S. Readers of this document are assumed to have sufficient knowledge to develop such applications (this knowledge is available in the user documentation provided with FeliCa Lite-S, the Reader/Writer, SDK, and so on).

The purpose of this document is to provide its readers with usage examples of FeliCa Lite-S, to present the relevant concepts of security, to warn you of potential problems during development, and so on in an easy-to-understand style.

This document does not guarantee flawless operation or defect-free security of the application. Neither does it cover all the specifications of each product. Therefore, for detailed specifications of other products you intend to use with FeliCa Lite-S, see the documentation supplied with them.

NOTE 1 In this document, conventional FeliCa cards are referred to as FeliCa Standard cards, to distinguish between conventional FeliCa cards and FeliCa Lite-S.

NOTE 2 For the differences in documentation between FeliCa Lite-S and FeliCa Lite, please see “Differences Between FeliCa Lite Documents and FeliCa Lite-S Documents”.

Contents

1 Applicable product

This document applies to the following product:

- IC Chip for Contactless IC card FeliCa Lite-S

2 Reference documents

This document includes references to the publications shown in the following table:

Table 2-1: Bibliography

Title	Document details
FeliCa Lite-S User's Manual	Published by Sony (http://www.sony.net/Products/felica/business/tech-support/index.html)
NFC Forum Type 3 Tag Operation Specification	Published by NFC Forum (http://www.nfcforum.org).

3 Example of FeliCa Lite-S usage

This chapter provides examples of FeliCa Lite-S usage.

3.1 Read-Only tag

FeliCa Lite-S can be used as a Read Only Tag. That is, data can be written only once, at the time of its issuance, after which the rewriting of data is prohibited.

3.2 Read-Write tag

FeliCa Lite-S can be used as a rewritable Read-Write Tag.

3.3 Multi-use ticket and one-time ticket

FeliCa Lite-S has a Subtraction Register Block function, which allows only the subtraction of data. Using this function, FeliCa Lite-S can be used as a multi-use ticket.

FeliCa Lite-S can be used as a one-time ticket if the value of this register is set to 1 at the time of issuance (and the total value is subtracted from it when it is used for the first time).

3.4 NFC Forum Type 3 Tag

FeliCa Lite-S can be used as an NFC Forum Type 3 Tag.

3.5 Card with authentication function

FeliCa Lite-S provides the Internal Authentication function that the Reader/Writer uses to authenticate the FeliCa Lite-S card, the External Authentication function that the FeliCa Lite-S card uses to authenticate the Reader/Writer, and the Mutual Authentication that is performed by combining the Internal Authentication and the External Authentication functions. By using these functions, either the Reader/Writer or the application can verify the authenticity of a card presented to the Reader/Writer. FeliCa Lite-S can verify the authenticity of either the Reader/Writer or the application and can allow only genuine entities to read and write.

3.6 Card with MAC-generation function

FeliCa Lite-S provides functionality to add a MAC (Message Authentication Code) to the data that is read from it. By verifying the consistency between the data that is read from FeliCa Lite-S and its MAC, either the Reader/Writer or the application can confirm that such data was not modified on the communication channel.

4 Identification of cards and applications

This chapter describes the important differences between FeliCa Lite-S and FeliCa Standard cards, so you can identify a card and its application.

4.1 IDm

IDm (manufacture ID) is the ID of 8 Bytes returned from a card in response to the Polling command.

IDm is set to identify the card during data communication. If two or more cards are present within the communication range of the Reader/Writer, the Reader/Writer uses IDm to identify and select the intended card for communication.

For FeliCa Standard card, IDm is also used to trace the cards manufactured by the manufacturer.

FeliCa Lite-S uses two types of identification data, as follows:

- IDm (manufacture ID), which is returned as the response to the Polling command
- Device ID (IDd), which is read from the device ID Block (D_ID).

IDm and IDd share the same value, which is written to enable manufacturers to trace their ICs after they are shipped from the factory.

4.2 Identification of application

In the operation of a system using FeliCa Standard card, applications are identified by using System Code. For FeliCa Lite-S, however, you are recommended to use Data Format Code (DFC) to identify its application.

DFC is the values of the 9th and 10th Bytes in the ID Block. DFC is written at the time of the issuance and cannot be rewritten after System Block is set to the rewrite prevention state.

Sony manages the assignment of every DFC.

For FeliCa Lite-S, unique values (i.e., 88B4h for FeliCa Lite-S and FeliCa Lite, or 12FCh for NFC Forum Type 3 Tag) are assigned to System Code. Therefore, System Code cannot be changed in accordance with the customer's application.

4.3 Usage as NFC Forum Type 3 Tag

If you use FeliCa Lite-S as an NFC Forum Type 3 Tag, see "NFC Forum Type 3 Tag Operation Specification" for details.

When you store any NDEF (NFC Data Exchange Format) record to a Type 3 Tag, you must set System Code to 12FCh, as described in "FeliCa Lite-S User's Manual".

5 Security

This chapter describes the security of any system constructed using FeliCa Lite-S, for your consideration.

5.1 Overview of security

In selecting security measures, it is important to understand the relationship between the cost of implementing the security measures and the effectiveness achieved by such security measures. To be more precise, first determine the value of the information assets to be protected. Next, assume the threats against the assets. Then, finally, substantiate the countermeasures against the threats.

The needs for costly countermeasures differ widely, depending on judgment of the value of the assets. Only the customer can pass such judgment. Therefore, it is the customer's responsibility to determine the system operation based on the level of security that is implemented.

While constructing a system, hierarchical structure such as "security function in higher-level application", "security attained by management of the system operation", and so on is assumed, together with the security functions of individual devices such as cards, the Reader/Writer, and so on. In this way, the security appropriate to the customer's usage of FeliCa Lite-S can be realized. Therefore, the customer must understand that the scope of security functions of such individual devices is limited.

Assuming full understanding of this situation, the customer is requested to construct and operate a system that has security functionality appropriate to the value of the information assets the customer intends to handle. To protect against widespread damage if one area of the security functionality becomes broken in the hierarchical structure, it is important that the customer decides during the construction and operation of the system which detection method and procedures apply.

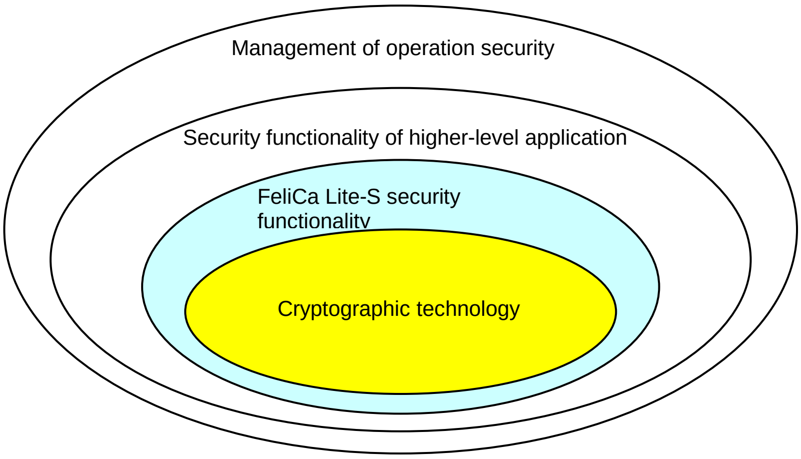
Management of operation security
Security functionality of higher-level application
FeliCa Lite-S security functionality
Cryptographic technology

Figure 5-1: Conceptual diagram of security functionality at each level of the application

5.2 Security in FeliCa Lite-S

FeliCa Lite-S, as well as FeliCa Lite, targets the handling of lower-value assets than those targeted by FeliCa Standard card. Based on this concept, FeliCa Lite-S realizes the benefits of low price and high level of usability by limiting the available security measures.

FeliCa Lite-S has the following security features, above FeliCa Lite:

- Write is allowed only if the attached MAC is correct (Write With MAC)
- Read is allowed only if the authentication has been successfully executed (Read After Authentication)
- Write is allowed only if the authentication has been successfully executed (Write After Authentication)

Table 5-1 shows the major differences in security between FeliCa Lite-S, FeliCa Standard card, FeliCa Lite, and generic magnetic cards.

Table 5-1: Major differences in security between FeliCa Lite-S and other cards

Security function	FeliCa Standard card	FeliCa Lite-S	FeliCa Lite	Generic magnetic card
Access control (Read)	Yes (authentication-required Service)	Yes (Read After Authentication)	No	No
Access control (Write)	Yes (authentication-required Service)	Yes (Read Only Service, Write With MAC, and Write After Authentication)	Yes (Read Only Service)	
Authentication function	Yes (Mutual Authentication)	Yes (Internal Authentication, External Authentication, and Mutual Authentication)	Yes (Internal Authentication = Unilateral Authentication)	No
Channel encryption function	Yes	No	No	No
MAC generation function	No	Yes	Yes	No
Tamper-resistance function	Yes (Security certified chip)	Yes	Yes	No

FeliCa Lite-S is designed to prevent unauthorized analysis.

However, for applications such as electronic money where a high level of security is required, you are strongly recommended to use FeliCa Standard card, which contains a security certified chip.

5.2.1 Internal Authentication (Unilateral Authentication function)

Using the Internal Authentication function (the Unilateral Authentication function) of FeliCa Lite-S, the Reader/Writer can verify that a card presented to it is the card in which a valid key is stored. For details of how to perform the Internal Authentication function, see "FeliCa Lite-S User's Manual".

5.2.2 External Authentication function

By using the External Authentication function of FeliCa Lite-S, the Reader/Writer can make FeliCa Lite-S authenticate the Reader/Writer in which a valid key is stored. To read or write User Block that is set as Read After Authentication or Write After Authentication, External Authentication shall be successfully performed beforehand. For details of how to perform the External Authentication function, see "FeliCa Lite-S User's Manual".

5.2.3 Mutual Authentication function

By using the Internal Authentication function and the External Authentication function of FeliCa Lite-S, the Reader/Writer and FeliCa Lite-S can verify that the other entity is a genuine device that has a valid key. For details of how to perform the Mutual Authentication function, see "FeliCa Lite-S User's Manual".

5.2.4 Access control

For FeliCa Lite-S, each User Block can be assigned the following access permissions:

- RW permission (to allow both the reading and writing of data) or RO permission (to allow only the reading of data)
- Write With MAC (to require MAC for the writing of data)
- Read After Authentication (to require successful External Authentication beforehand for the reading of data)
- Write After Authentication (to require successful External Authentication beforehand for the writing of data)

5.2.5 MAC-generation function

Using the MAC-generation function of FeliCa Lite-S, you can detect whether the data read from FeliCa Lite-S was modified on the communication channel. For details of how protect such data with the MAC-generation function, see "FeliCa Lite-S User's Manual".

5.2.6 Assumed attacks and countermeasures

The following table shows the assumed attacks in the environment where FeliCa Lite-S is used; it also shows the countermeasures to address those attacks:

Table 5-2: Assumed attacks and countermeasures

Assumed attacks	Countermeasures
Unauthorized card may pretend to be genuine.	Use the Internal Authentication function.
Data stored in the card may be overwritten with commands by an unauthorized user.	Set Block as Write After Authentication or Write With MAC.
A command for writing data may be modified during communication, and then modified data is written to the card.	Set Block as Write With MAC.
Data read from the card may be modified during communication.	Read With MAC and verify the MAC.
Data read from the card may be eavesdropped during communication.	Read and Write encrypted data by the Reader/Writer or the application. (See section 5.4.1 “Confidentiality”)

5.2.7 MAC Block and MAC_A Block

MAC_A Block, which is added to FeliCa Lite-S, provides the following features compared with MAC Block.

- When Read With MAC is executed, Block Number is included in the MAC generation.
- When Write With MAC is executed, Block Number and the write counter are included in the MAC generation.

MAC Block is generated only from the read data. Therefore, countermeasures by the application are recommended to detect the unauthorized modification of the command so that the data is read from Block other than the one specified. On the other hand, MAC_A Block is generated from the read data and Block Number. Therefore, if the command is modified so that the data is read from Block other than the one specified, MAC verification process returns an error to signal that the command has been modified.

For the Write With MAC function, the write counter is included in the MAC generation, in addition to the read data and Block Number. This prevents any replay attack (i.e. retransmission of the valid command to execute the Write With MAC operation) by detecting that the write counter is not incremented.

Although FeliCa Lite-S supports MAC Block to maintain the compatibility with FeliCa Lite, you are recommended to use MAC_A Block, which enforces security.

5.3 Cautions on card keys

This section describes specific cautions on card keys.

5.3.1 Management of card keys

To protect card keys from leakage of information and from loss, be especially careful when handling them.

The card key is set at the time of card issuance. Issuance of cards should be done in a secure environment, taking into consideration the risk of interception (eavesdropping) of wireless communication.

5.3.2 Generation of card keys

For card keys, you should set diversified keys so that no card shares the same key values.

For card keys that were set so that they have different values per card, a card key for a specific card cannot be used as the card key for other cards, even if such a card key was analyzed and the key information leaked. In this way, you can minimize risk.

For details of how to generate card keys, see “FeliCa Lite-S Diversified Card Key Standard Generation Algorithm”.

5.4 Security at application levels

5.4.1 Confidentiality

If the user data is not set as Read After Authentication, anybody can read the user data stored in FeliCa Lite-S. When you want to restrict reading permission to the genuine Reader/Writer of the application, the user data should be set as Read After Authentication. In addition, eavesdropping of the wireless communication channel is possible because the communication channel is not encrypted. To prevent eavesdropping, data should be encrypted by either the Reader/Writer or the application before the data is stored in FeliCa Lite-S. For a conceptual diagram of this procedure, see Figure 5-2.

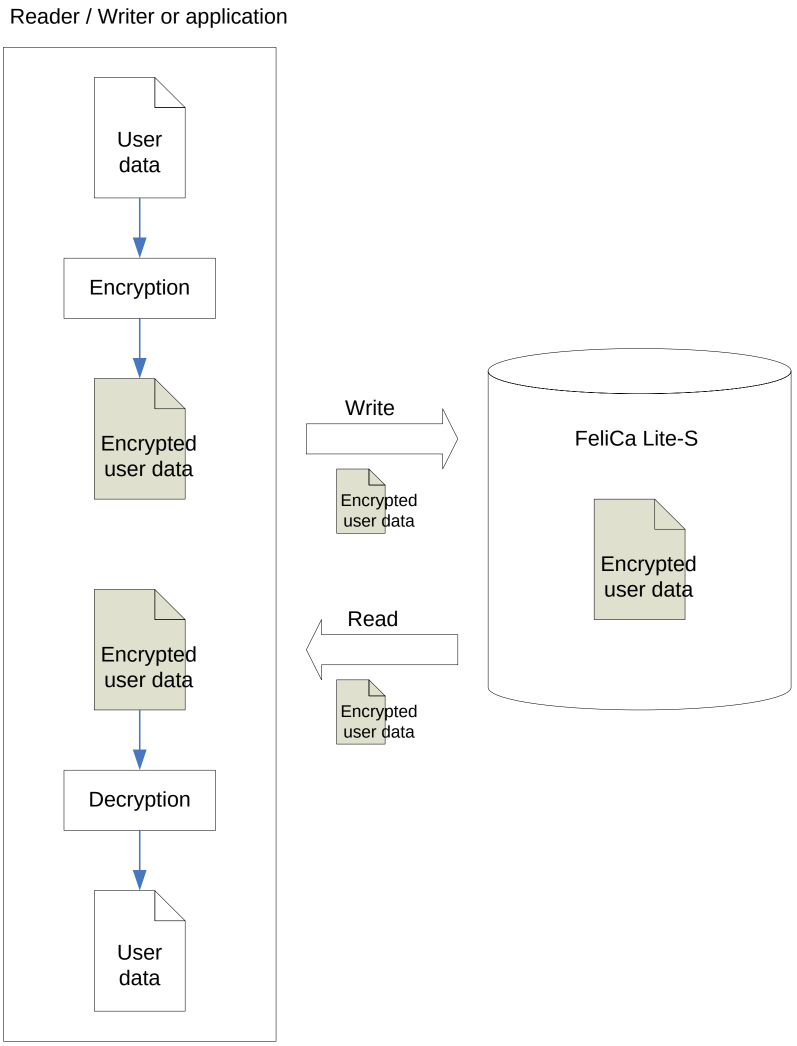

Figure 5-2: Example operation to protect the confidentiality of user data

If you use encryption / decryption keys that differ per card, the encrypted user data on each card becomes different. By using this procedure, you can prevent encrypted card data that was read from one card from being reused with another card.

For information about the handling and diversification of the key, see section 5.3 "Cautions on card keys".

5.4.2 Integrity

Unless the user data is set as RO permission or Write After Authentication, anybody can, without authentication, rewrite the user data stored in FeliCa Lite-S. Even if the user data is set as Write After Authentication, there is a risk that the wireless communication data can be modified, because the communication channel is not encrypted. The wireless communication data can be modified in any of the following cases:

- The data to be written to FeliCa Lite-S is modified.
- The data read from FeliCa Lite-S is modified.
- The write command is modified so that the data is written to Block other than the one specified.
- The read command is modified so that the data is read from Block other than the one specified.

To prevent these attacks, you should use the Read With MAC and Write With MAC functions.

For further protection of the integrity of data, you are recommended to have the Reader/Writer or the application generate and store the signature together with the data.

In addition, to detect the replacement of Block to which the data is written or from which the data is read, you are recommended to insert an identifier into Block Data (such as Block Number).

As in the preceding section, use the diversified keys to generate the signature. This makes the signature and MAC for the same data different per card. With this procedure, you can prevent abuse of a card to which the data plus signature read from a different card is written.

For details of the handling and diversification of the key, see section 5.3 "Cautions on card keys".

The summary of examples of countermeasures is shown in Table 5 3.

For conceptual diagrams of the previously-described procedures, see Figure 5 3 (which shows only the protection of integrity) and Figure 5 4 (which shows a combination of protection of both integrity and confidentiality).

Table 5-3: Summary of examples of countermeasures

Assumed attack	Example of countermeasure by FeliCa Lite-S	Example of countermeasure by the application
The data to be written to FeliCa Lite-S is modified.	Use the Write With MAC function (MAC_A Block).	Generate and store the signature.
The data read from FeliCa Lite-S is modified.	Use the Read With MAC function (MAC_A Block).	Generate and store the signature.
The write command is modified so that the data is written to Block other than the one specified.	Use the Write With MAC function (MAC_A Block).	Generate and store the signature. Insert an identifier (such as Block Number).
The read command is modified so that the data is read from Block other than the one specified.	Use the Read With MAC function (MAC_A Block).	Generate and store the signature. Insert an identifier (such as Block Number).

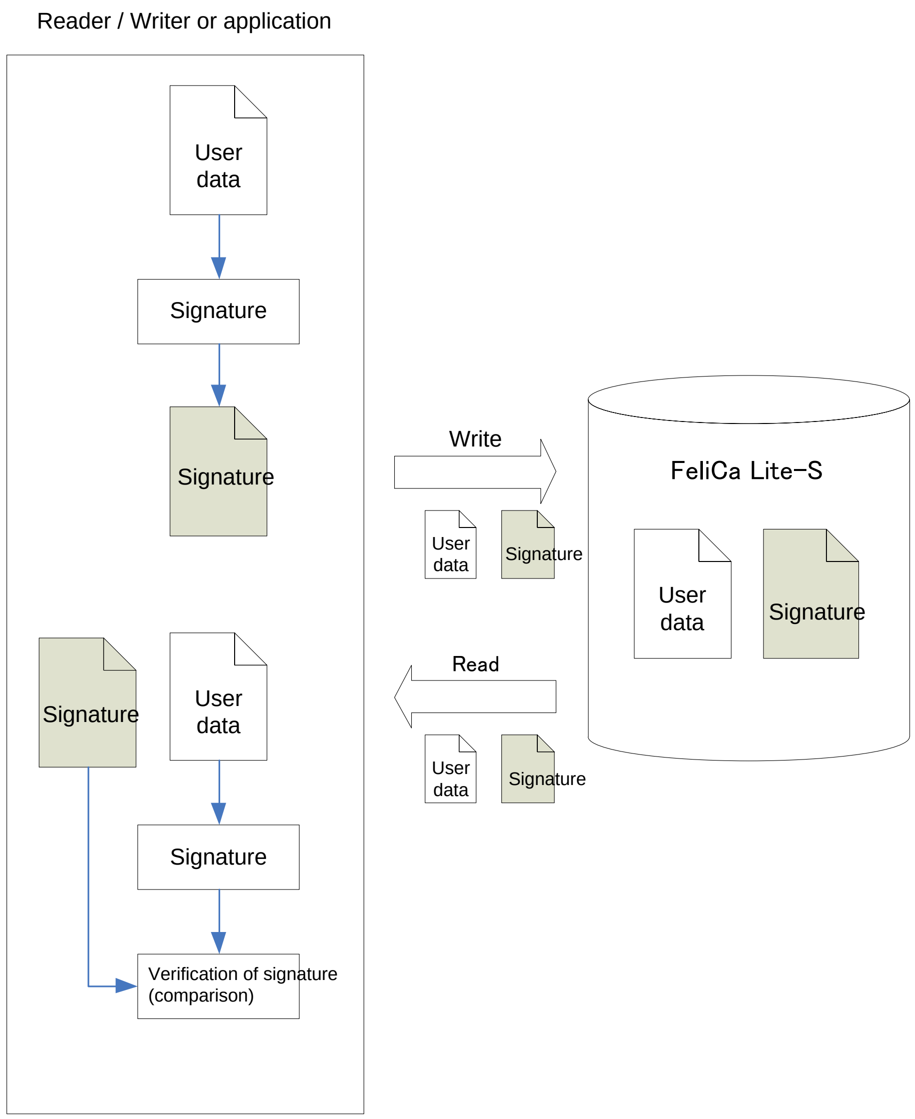

Figure 5-3: Example of integrity protection by assigning a signature

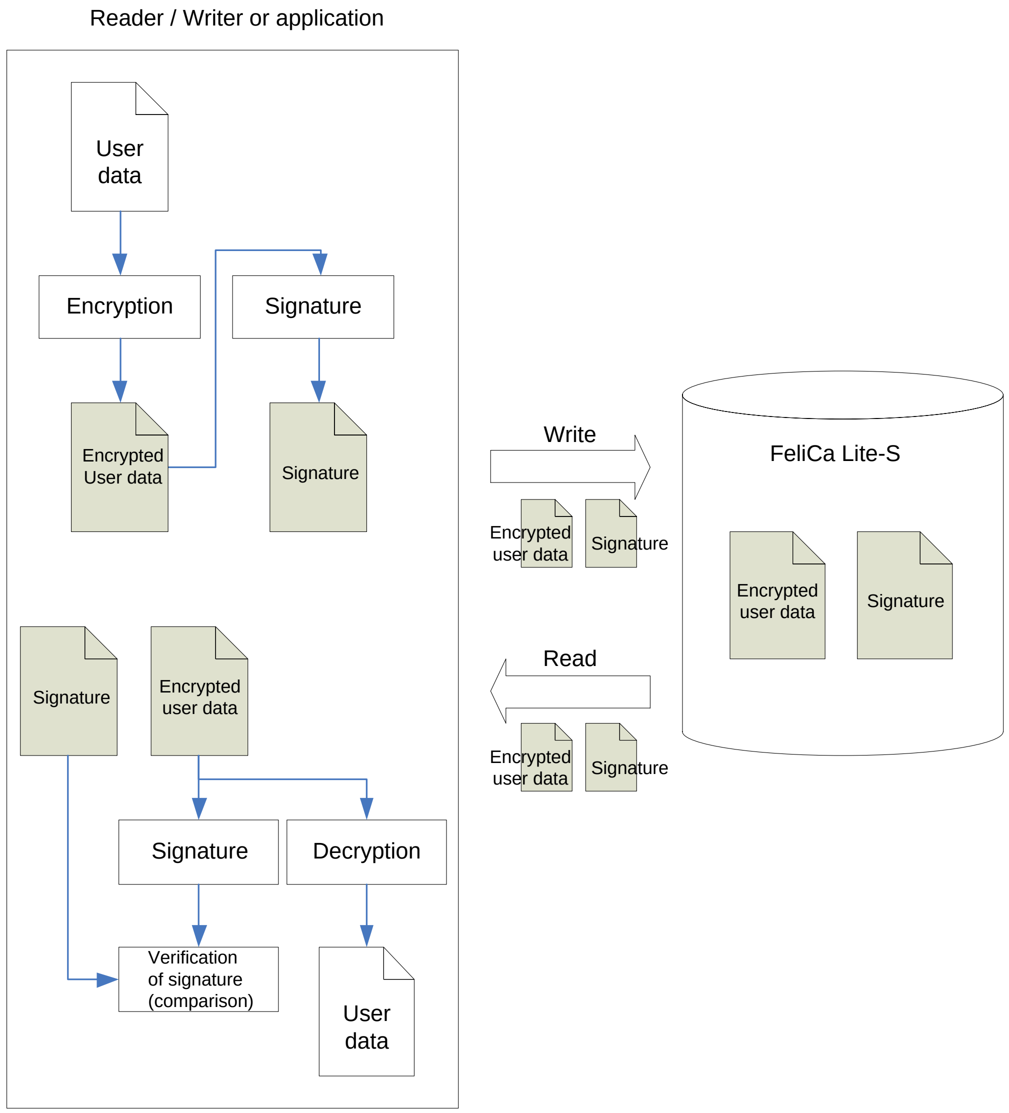

Figure 5-4: Example of how to protect confidentiality and integrity by data encryption and assignment of signature

5.5 Cautions on security

This section describes notable aspects of FeliCa Lite-S security.

5.5.1 Random number generated by the Reader/Writer

The session key used for the Internal Authentication, the External Authentication, the Mutual Authentication, Read With MAC, and Write With MAC is generated based on the secret card key and on the random number written by the Reader/Writer. By keeping the card key to be used secret, the session key becomes difficult to guess. By changing the random number generated by the Reader/Writer for each session, the session key changes for each session and can be used as a single-use key.

If the random number was not rewritten, the MAC value reverts to what it was at the previous authentication. In this situation, you can authenticate an imposter (impersonated) card. Therefore, when using the Unilateral Authentication function, make sure you write a different random number immediately before each session.

Figure 5-5 illustrates the relationship between random number and MAC mentioned in this section.

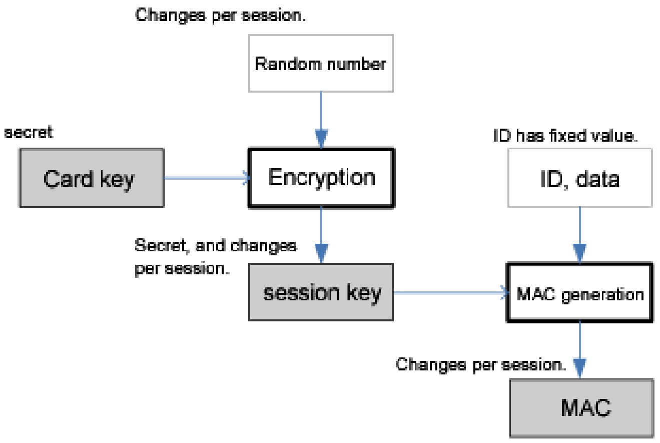

Figure 5-5: Relationship between random number and MAC

5.5.2 Protection from tampering

FeliCa Lite-S is designed to prevent unauthorized analysis.

However, for applications (such as electronic money) that are probably exposed to such high-level attacks, you should use FeliCa Standard card products. FeliCa Standard card products were evaluated for security by a third-party evaluation body, and awarded security certifications from official agencies.

5.5.3 Security in the Reader/Writer and in higher-level systems

Considering the security, it is important to pay attention to FeliCa Lite-S, the Reader/Writer, and higher system levels provided by the customer.

Section 5.3.2 "Generation of card keys" in this document introduces the concept and practice of card-key diversification. The secret key (to be used as the master key for diversification) and the diversification algorithm are stored either in the Reader/Writer or in the higher-level application. If the secret key or the diversification algorithm is analyzed and the information leaked, adverse effects can spread throughout the system.

Therefore, users of FeliCa Lite-S are requested to implement the appropriate security measures, taking the value of asset handled by the user's service and the significance of security threats into consideration.

5.5.4 Cautions for changing the card key

The card key in FeliCa Lite-S can be changed by using the Write With MAC function. If the communication is eavesdropped, the new key value is leaked because the data written as the new key is not encrypted during the Write With MAC operation. Therefore, the operation to change the card key should be performed in a secure environment where the communication channel is protected from eavesdropping.

This function can be applied whenever a multi-use ticket or a single-use ticket is collected, has its card key changed, and is then reused. Therefore, it is assumed that the operation to change the card key is performed either in an issuing facility, or using issuing equipment, or both.

If you do not change the card key, the card key should be set as Read Only in the 1st issuance procedure.

FeliCa Lite-S

FeliCa Lite-S Security Application Note Version 1.11

March 2012	First Edition	FeliCa Business Division
April 2017	Revision	

Sony Imaging Products & Solutions Inc.

No. M743-E01-11