SONY

FeliCa Standard

FeliCa Card
Command Sequence
Design Guidelines

Version 1.02

No. M620-E01-02

Introduction

This document describes the command sequences assumed in the design of applications that utilize FeliCa technology, such as electronic money services, authentication services, and so on.

The intended audience of this document is engineers engaged in development of the Reader/Writer and applications for FeliCa card. It is assumed that readers of this document have an appropriate level of knowledge and understanding of the terminology used both in FeliCa technology and in general software development work.

If you have any questions about the development of application software that is compatible with mobile FeliCa cards, please contact FeliCa Networks, Inc. (info-fn@FeliCaNetworks.co.jp).

This document provides guidelines for designing a command sequence for common use; it is not intended for mandatory implementation. Customers are requested to design a proprietary command sequence that best fits the relevant operating environment and application, while referring to the content of this document.

The content of this document does not guarantee the correct operation of the system with all existing or future FeliCa cards.

Contents

1 Basic command sequence (success scenario)

This chapter describes the basic command sequence for FeliCa commands.

The basic command sequence is the one to be assumed in general secure applications. It starts from the acquisition of a card, and includes identification of Service, mutual authentication, and read or write of data with encrypted communication.

In the basic command sequence (success scenario), it is assumed that the execution of commands is performed in the following order:

1) Acquisition of card

   This step executes the Polling command to which a system code is specified, and acquires Manufacture ID (IDm) as the card identification information.

2) Verify existence of Service

   This step checks for the existence of the Service to access, by using the Request Service command, while specifying IDm acquired by the Polling command. If the Service exists, the key version of the Service is returned in response to the Request Service command.

3) Mutual authentication

   This step executes the Authentication1 and Authentication2 commands to the Area / Service to be accessed, and performs mutual authentication.

4) Readout of block data

   This step executes the Read command, and then reads the block data from the authenticated Service. This step assumes the block data is checked to determine which data to write in the subsequent process (for example, the remaining balance in an electronic money service).

5) Verify existence of card

   This step executes the Request Response command to check for the existence of the card. In an application that utilizes contactless IC cards, in some cases the response returned from the card might become unavailable because either the command or the response does not reach the intended destination or because the card is moved beyond the communication range of the Reader/Writer. Therefore, it is recommended to write block data immediately after reconfirming that communication with the card is possible. This is the most important process in the basic command sequence (for example, for a charge process or a decrement process of an electronic money service). For a detailed explanation of the effectiveness of the Request Response command, see Chapter 3 “Error handling during read or write of block data".

6) Writing of block data

   This step executes the Write command to write block data to the authenticated Service.

Figure 1-1 shows an example of a command sequence in a success scenario.

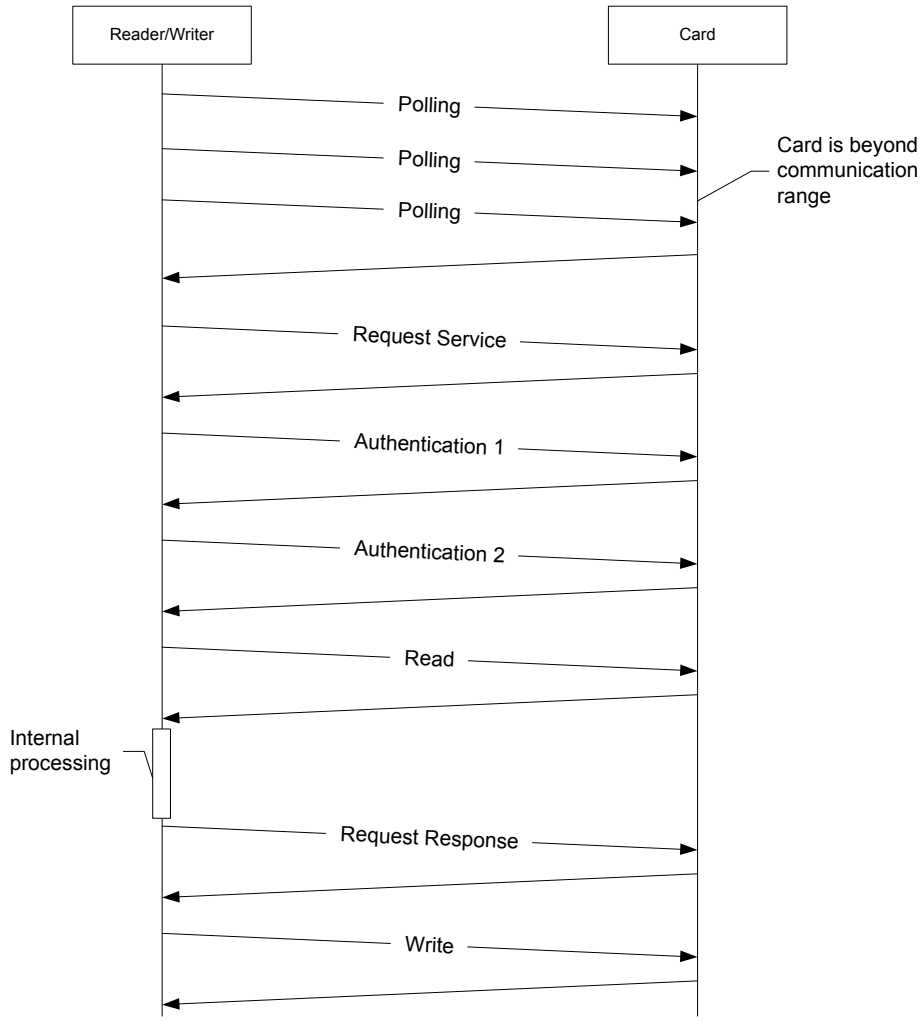

Figure 1-1: Basic command sequence (success scenario)

2 Error handling during mutual authentication

This chapter describes how to recover from abnormal behavior, specifically when no response is received from a card while attempting mutual authentication.

If no response is received from a card during mutual authentication, any of the following causes can be assumed:

- The card was unable to receive the command correctly because of communication breakdown.
- The command was executed correctly but the response does not reach the Reader/Writer due to communication breakdown.
- The command reached the card but the card does not return a response because the mode of the card switches to Mode0 as a result of power interruption.

  NOTE In the case of "power interruption", it is assumed that there can be a zone in the communication range of the Reader/Writer where electrical power is unavailable when the card is moved horizontally while it is presented to the Reader/Writer and, as a result, power interruption can occur when the card passes through such a zone.
- The command did not reach the card because the card was moved beyond the communication range.

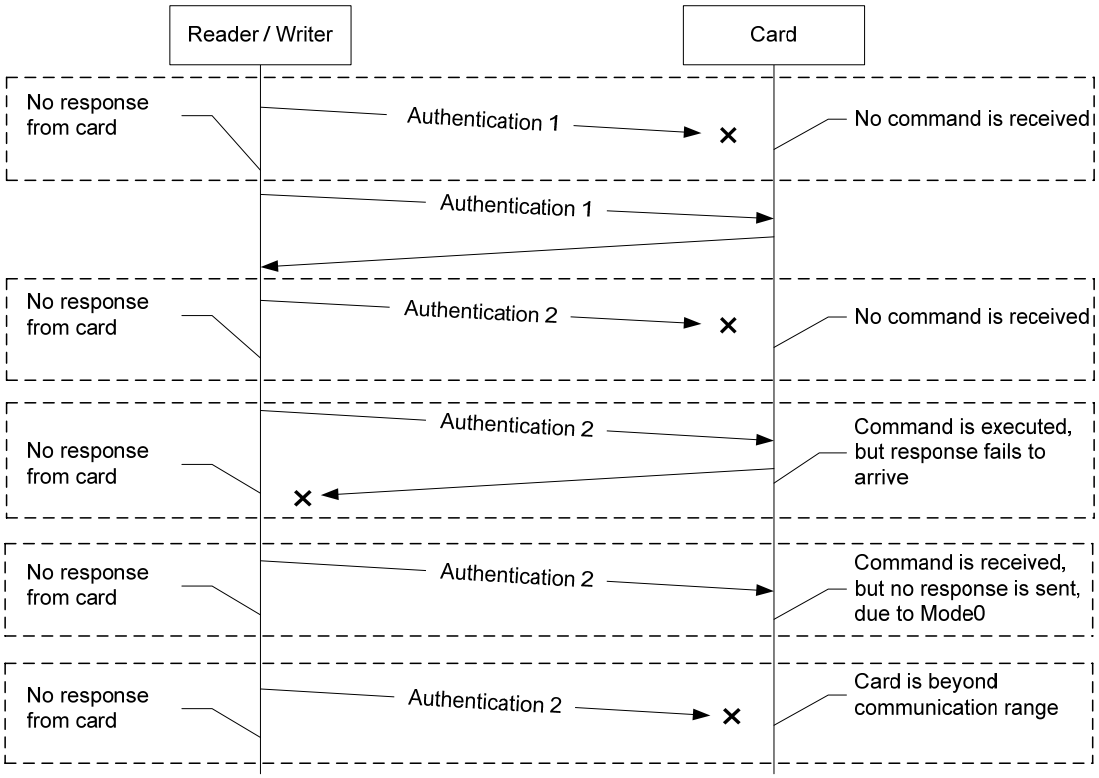

Figure 2-1: Assumed error occurrence during mutual authentication

If the abnormality is caused by communication trouble, recovery is possible by retransmitting the command. In the case of power interruption or if the card moves beyond the communication range, however, recovery from the abnormality is impossible even if the command is retransmitted. In both cases, the cause of the trouble is difficult to determine because, as far as the Reader/Writer is concerned, response from the card is simply unavailable.

In this recovery procedure, perform the mutual authentication process in the following order:

1) Transmit the Authentication1 command to the card.
2) If a response is returned from the card, proceed to step 3.

   If no response is returned, resend the Authentication1 command.

   If no response is returned to the second transmission of the Authentication1 command, either terminate the procedure in "Communication not completed" status, or return to the Polling process.
3) Transmit the Authentication2 command to the card.
4) If a response is returned from the card, terminate the procedure in "Communication successfully completed" status.

   If no response is returned, resend the Authentication2 command.

   If no response is returned to the second transmission of the Authentication2 command, proceed to step 5.
5) Transmit the Request Response command to the card.
6) If a response is returned from the card, proceed to step 7.

   If no response is returned, very probably the card has been moved beyond the communication range. In this case, either terminate the procedure in "Communication not completed" status, or return to the Polling process.

7) If the mode of the card is Mode0, it is highly likely that a power interruption occurred. In this case, repeat the mutual authentication process from transmission of the Authentication1 command in step 1.

   If the mode of the card is either Mode1 or Mode2, repeat the mutual authentication from the transmission of the Authetnication2 command in step 3.

Here follows a summary of the recovery procedure described in the previous list:

- If the abnormality occurred while the Authentication1 command was being processed, retransmission of the command is tried first, in case the problem was caused by poor communication. If no response is returned to the retransmitted command, it is assumed that the card was moved beyond the communication range. Either the procedure is terminated in "Communication not completed" status, or acquisition of the card is tried again by using the Polling command.
- If the abnormality occurred while the Authentication2 command was being processed, retransmission of the command is tried first. If no response is returned to the retransmitted command, the Request Response command is transmitted to verify the existence of the card. If no response is returned to the Request Response command, it is assumed that the card was moved beyond the communication range. Either the procedure is terminated in "Communication not completed" status, or acquisition of the card is tried again by using the Polling command. If a response is returned, the procedure depends on the current mode of the card. If the card is in Mode0, authentication is performed again from transmission of the Authentication1 command, because the possibility of power interruption is high. If the card is in Mode1 or Mode2, authentication is performed again from transmission of the Authentication2 command, because the status of normal completion of the Authentication1 command is maintained.

Figure 2-2 shows the recommended procedure for recovery from abnormal behavior during mutual authentication.

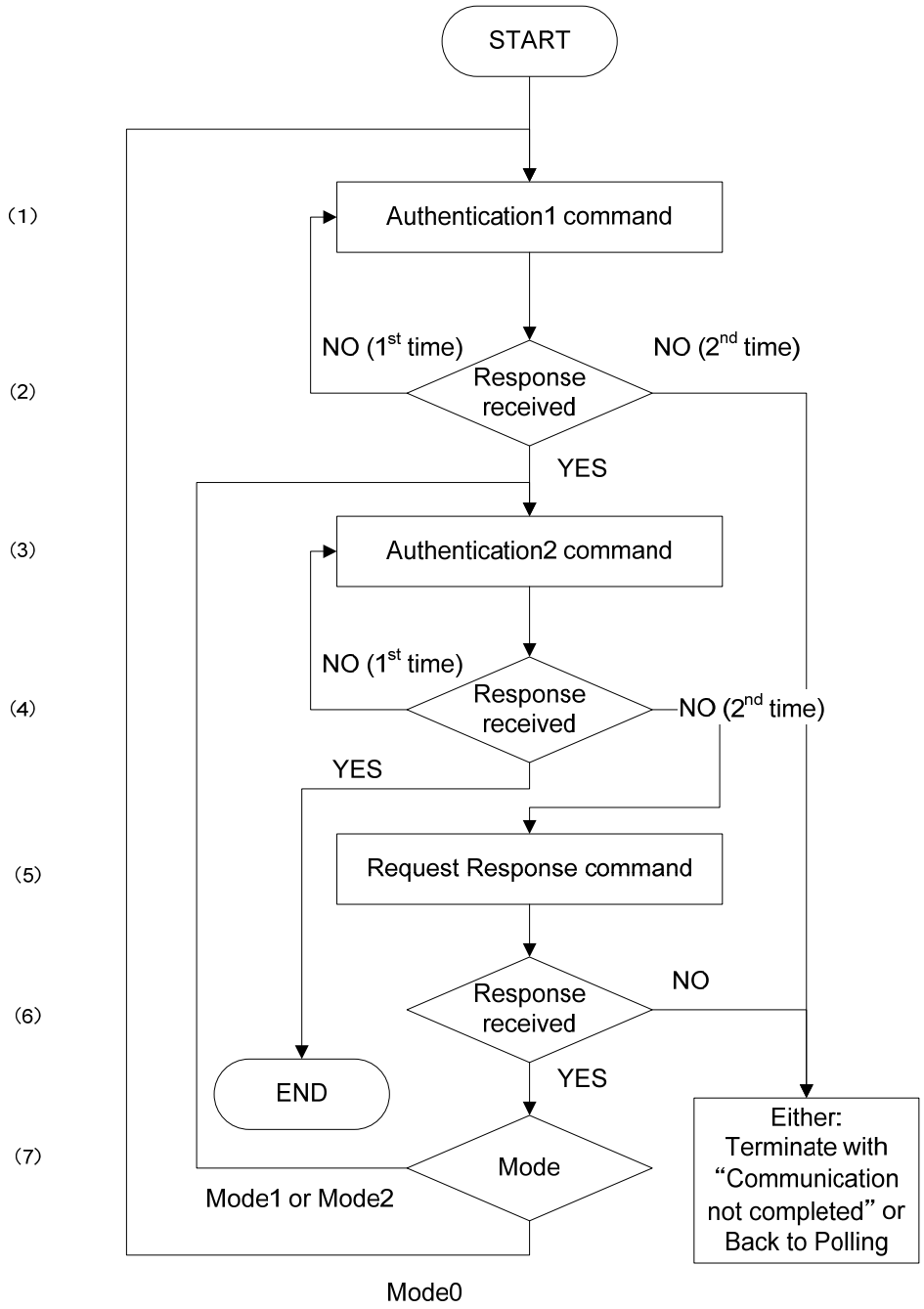

Figure 2-2: Recovery procedure from Error Occurrence during Mutual Authentication

3 Error handling during read or write of block data

This chapter describes how to recover from abnormal behaviour where no response is available from the card while attempting to read or write block data.

If no response is received from a card while attempting to read or write block data, any of the following causes can be assumed:

- The card was unable to receive the command correctly due to communication trouble (case (A) of Figure 3-1).
- The command was executed, but the response does not reach the Reader/Writer due to communication breakdown (case (B) Figure 3-1).
- The command reached the card but the mode of the card switches to Mode0 due to power interruption, resulting in no response (case (C) of Figure 3-1).
- The command did not reach the card because the card was moved beyond the communication range (case (D) of Figure 3-1).

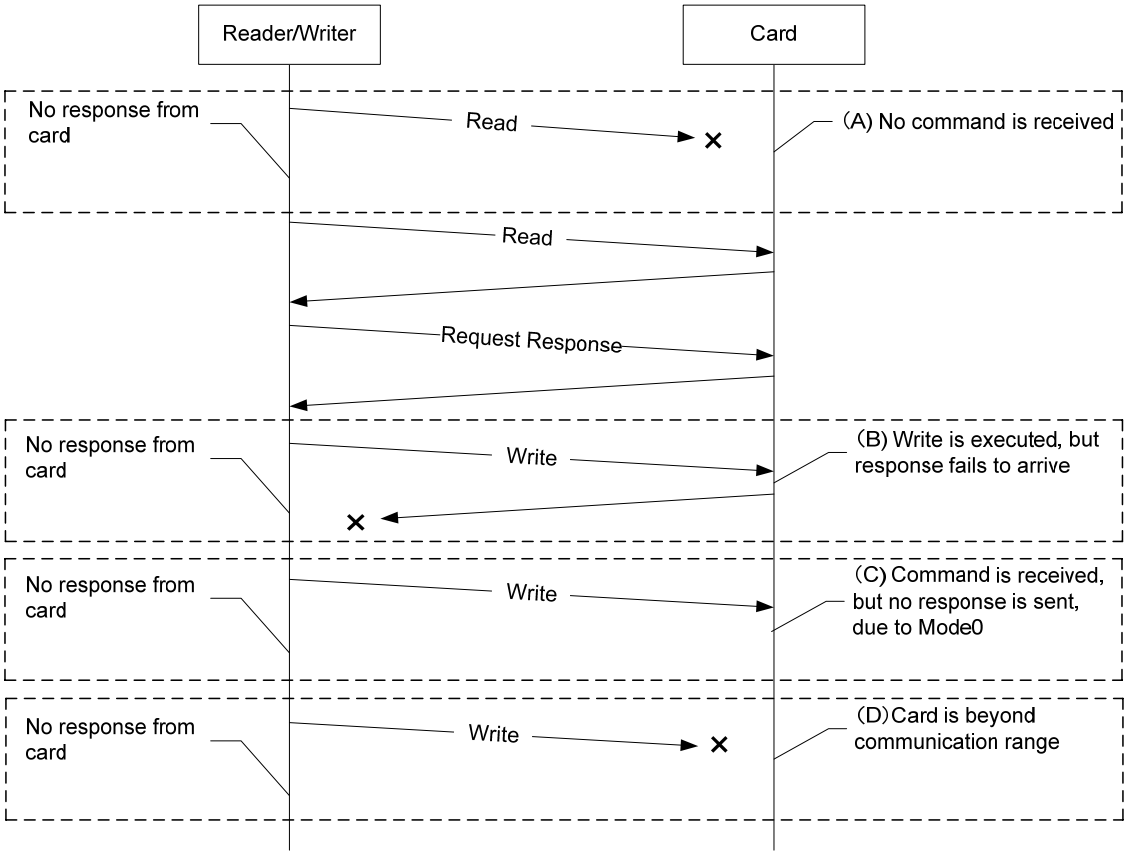

Figure 3-1: Assumed Error Occurrence Case during Read/Write

If the cause of the abnormality is communication trouble, recovery is possible by retransmitting the command. In the case of power interruption or if the card was moved beyond the communication range, however, recovery is impossible even if the command is retransmitted; in both these cases, the cause of the abnormality is difficult to determine because as far as the Reader/Writer is concerned the card is simply unavailable.

Figure 3-2 shows the recommended method for recovery from abnormal behavior during the execution of the Read/Write command. Perform the data read and data write processes in the following order:

1) Transmit the Read command to the card.
2) If a response is received from the card, proceed to step 3.

   If no response is received, resend the Read command.

   If no response to the second transmission of the Read command is received, either terminate the procedure in "Communication not completed" status or return to the Polling process.
3) Transmit the Request Response command to the card.
4) If a response is returned from the card, proceed to step 5.

   If no response is returned, it is highly likely that the card was moved beyond the communication range. In this case, either terminate the procedure in "Communication not completed" status, or return to the Polling process.
5) If the mode of the card is Mode0, it is highly likely that a power interruption occurred. In this case, either terminate the procedure in "Communication not completed" status, or return to the Polling process.

   If the card is in Mode2, proceed to step 6.
6) Transmit the Write command to the card.
7) If no response is received, retransmit the Write command.

   If no response to the second transmission of the Write command is received, it is highly likely that the card was moved beyond the communication range. In this case, either terminate the procedure in "Communication not completed" status, or return to the Polling process.

In the recovery process described in the previous list, retransmission of the command is performed first if any abnormality occurred, taking the possibility of communication trouble into consideration. If no response to such a retransmitted card is received, it is assumed that the card was moved beyond the communication range and the procedure is either terminated in "Communication not completed" status, or the Polling process is restarted in an attempt to acquire the card.

Note During the process of decrementing the remaining amount of funds in electronic money applications, repeated execution of the decrement process can be prevented by the Execution ID function of the Purse Service, even if the Write command is retransmitted.

During steps 3 to 5 of the previous process, the Request Response command is transmitted immediately before the Write command is executed, to verify the existence of the card. In the case of electronic money applications, for example, there is a chance that the card has moved beyond the communication range because some steps of the process are somewhat lengthy. For example:

a) Reads the data, using the Read command.
b) Checks that the remaining amount of funds is sufficient for payment.
c) Prepares decrement data, log data, and so on.
d) Finally, writes data (using the Write command).

If the Write command is transmitted while the card is moved beyond the communication range, no response is returned from the card, and the Reader/Writer is unable to determine whether the card

received the Write command and the decrement of money was performed or the card did not exist and the decrement of money was not performed. To minimize the risk of such a troublesome situation occurring, first verify the existence of the card by executing the Request Response command immediately before executing the Write command.

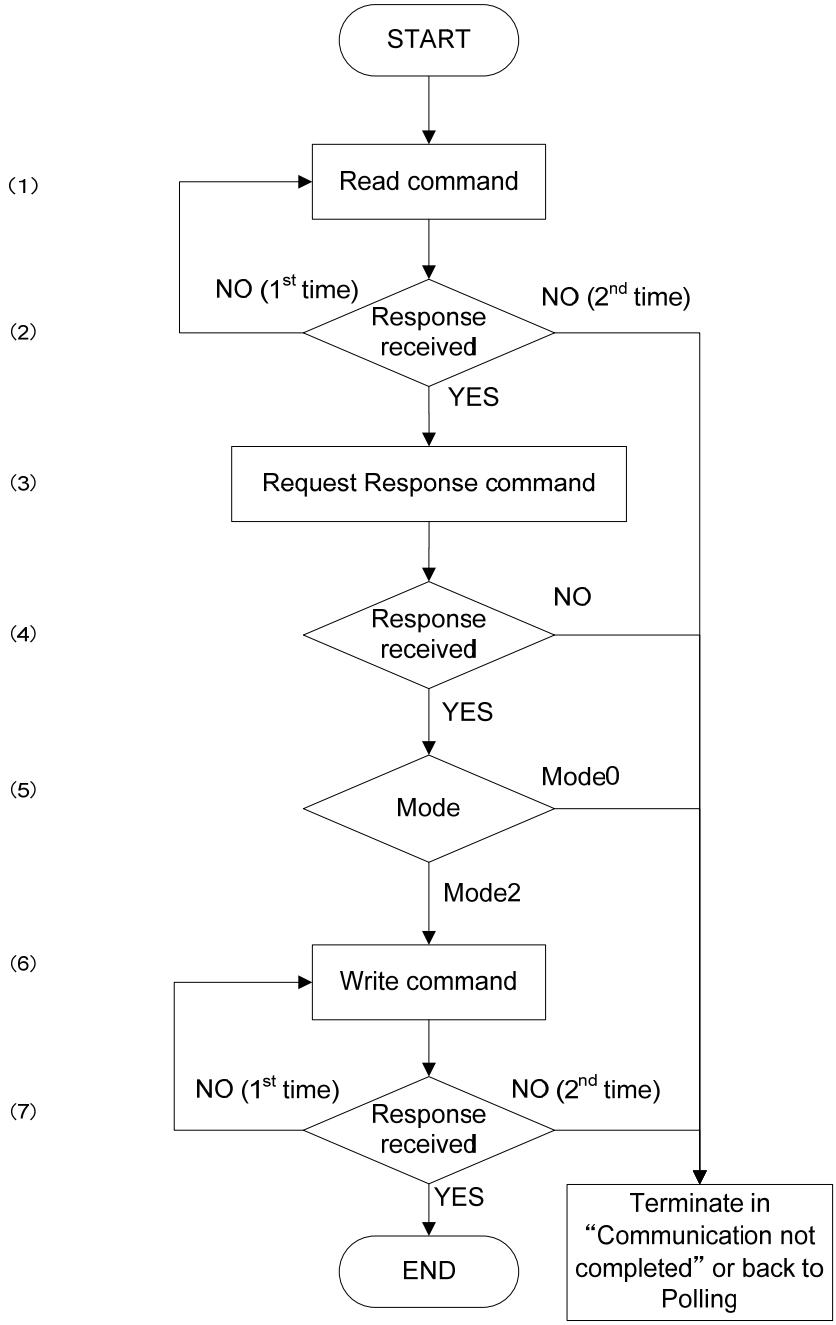

Figure 3-2: Recovery Procedure from Error Occurrence during Read/Write

FeliCa Standard

FeliCa Card Command Sequence Design Guidelines Version 1.02

July 2010	First Edition	FeliCa Business Division
April 2021	Revision	

Sony Corporation

No. M620-E01-02

Printed in Japan