4.5 ebMS Processing Mode

4.5.1 Outline of processing mode

Figure 4.5.1 shows outline of ebMS processing mode in NACCS.
When using this processing mode, it is necessary to incorporate server certificate and certificate for electronic signature which are provided by the NACCS Center into the user's ebMS server.
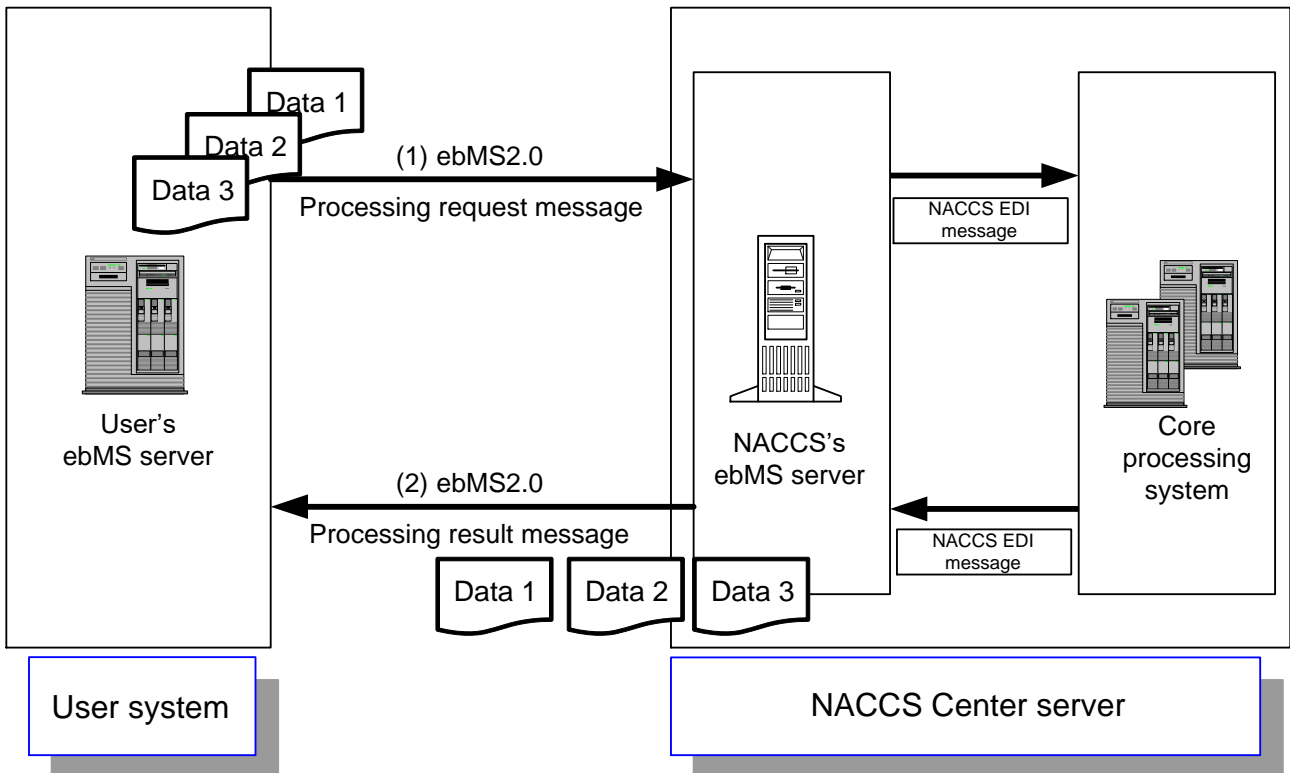For sending e-mail, refer to "4.6.1 e-mail".

Figure 4.5.1 Outline of ebMS Processing Mode

(1) A user creates and sends a NACCS EDI message or a XML message that contains necessary data segments for a transaction from the user system to the NACCS's ebMS server over HTTPS protocol.

(2) The message transmitted to the NACCS's ebMS server is transferred to the core processing system. The message is processed and a response message is sent to the NACCS's ebMS server once again. NACCS's ebMS server returns a processing result message to the user system over HTTPS protocol. Therefore, the user system should always be activated.

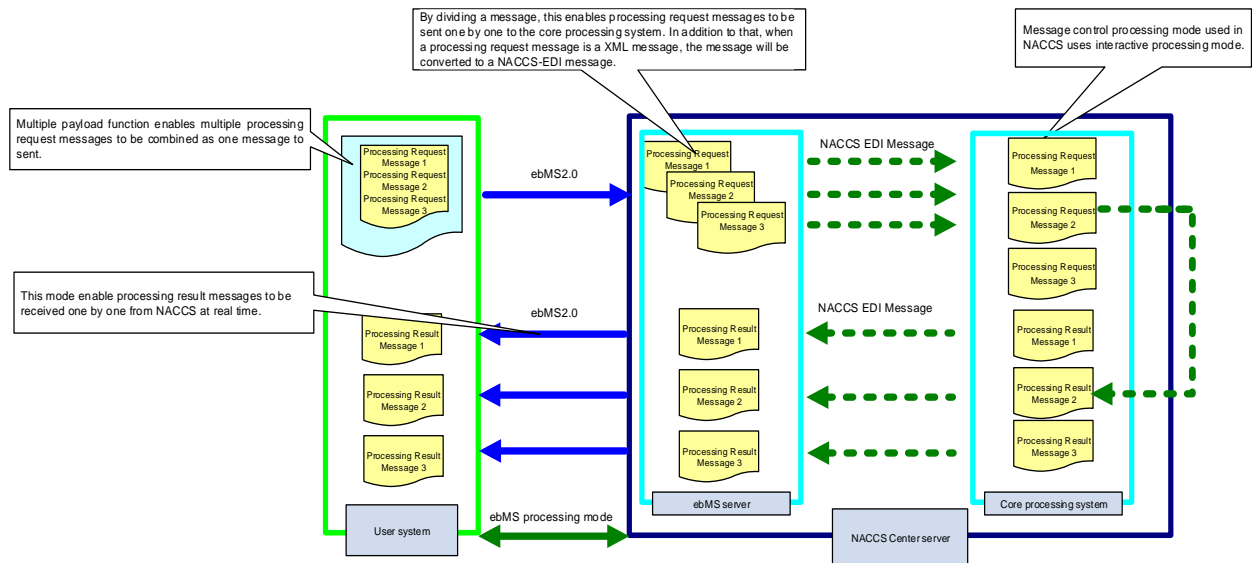In addition, Figure 4.5.2 shows outline of ebMS function.

Figure 4.5.2 Outline of ebMS Processing Mode

4.5.2   Details of the communications protocol

For communications protocol used in ebMS processing mode, TCP/IP is used for the network and transport layers, and HTTPS for the upper layers, and data transmission/receiving is carried out using ebMS2.0. In addition, multiple blocks of data can be transmitted in a batch.[1]

In addition, in NACCS, when a s multiple payload function is used, the maximum message length should be 10 MB (the same as EDIFACT multiple B/L message length), and the maximum number of messages for payload should be 99 messages (according to NACCS EDIFACT protocol).

Also, when using a multiple payload function, avoid a mixture of NACCS-EDI messages and XML messages.

(1)   Outline of ebMS2.0
For ebMS processing mode used in ebMS server, ebXML Message Service v2.0 (ebMS2.0) and ebXML CPPAv2.0 are used.
ebMS (ebXML Message Service) refers to specifications of transmission of messages used for electronic commerce between companies via Internet. This is composed based on SOAP. In ebMS processing mode, user carries out communication using CPA distributed by the NACCS Center. (For details of CPA, refer to "4.5.4 (3) Setting of CPA")

For details of ebXML Message Service v2.0 (ebMS2.0) and ebXML CPPA v2.0, refer to the following specifications opened to the public by OASIS[2].

• ebXML Message Service Specification v2.0, OASIS Standard
(http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf)
• ebXML CPPA v2.0, OASIS Standard
(http://www.oasis-open.org/committees/ebxml-cppa/documents/ebcpp-2.0.pdf)

Table 4.5.1 shows the list of functions of ebMS2.0 used in ebMS processing mode.

---

[1] When sending multiple processes all together, the multiple payload function of ebMS2.0 is necessary.
[2] Organization which carries out activities to promote standard technologies for XML (http://www.oasis-open.org/) and specified ebXML.

Table 4.5.1 List of Functions of ebMS processing mode

ebMS function	Description of function	ebMS Processing Mode	Remarks
Security(TLS)	Is TLS used for communication?	Used	Only server authentication is used
Security(Signature)	Is digital signature used in communication?	Used	XML signature (digital signature in XML format)
Error Handling	Is error response returned during error?	Used	Errorlist
SyncReply (synchronized response)	For return of Acknowledgment (acknowledgment of receipt), is it returned in the same session as that of ebXML received?	Not used	Asynchronous response mode (Acknowledgment is sent in separate session)
Reliable messaging	Are systems such as acknowledgment of receipt, retry, and de-duplication used?	Used	High-reliability messaging
MessageStatusService	Is inquiry about message status used?	Not used	
MSH Ping Service	Is inquiry about status of ebMS execution modules used?	Not used	
MessageOrder	Is arrival order at message sender side guaranteed? (used when the sender's system has multiple ebMSs)	Not used	
Multi-Hop	Is data transfer between multiple servers used?	Not used	

4.5.3　Messages used in ebMS processing mode

ebMS processing mode carries out transmission/receipt processes using high-reliability messaging provided by ebMS2.0.

(1)　Messages used in ebMS processing mode
The following shows ebMS messages used in ebMS processing mode.

- Application messages
Processing request message and processing result messages, etc.

- ebMS receipt confirmation message (Acknowledgement)
Confirmation of receipt of messages in ebMS processing mode

- ebMS error notification message (ErrorList)
Notification of error in ebMS processing mode

(2) ebMS2.0 Message format

ebMS2.0 message format is regulations where SOAP message is extended. In addition, execution module which mounts ebXML Message Service specifications is called ebXML MSH (message service handler).
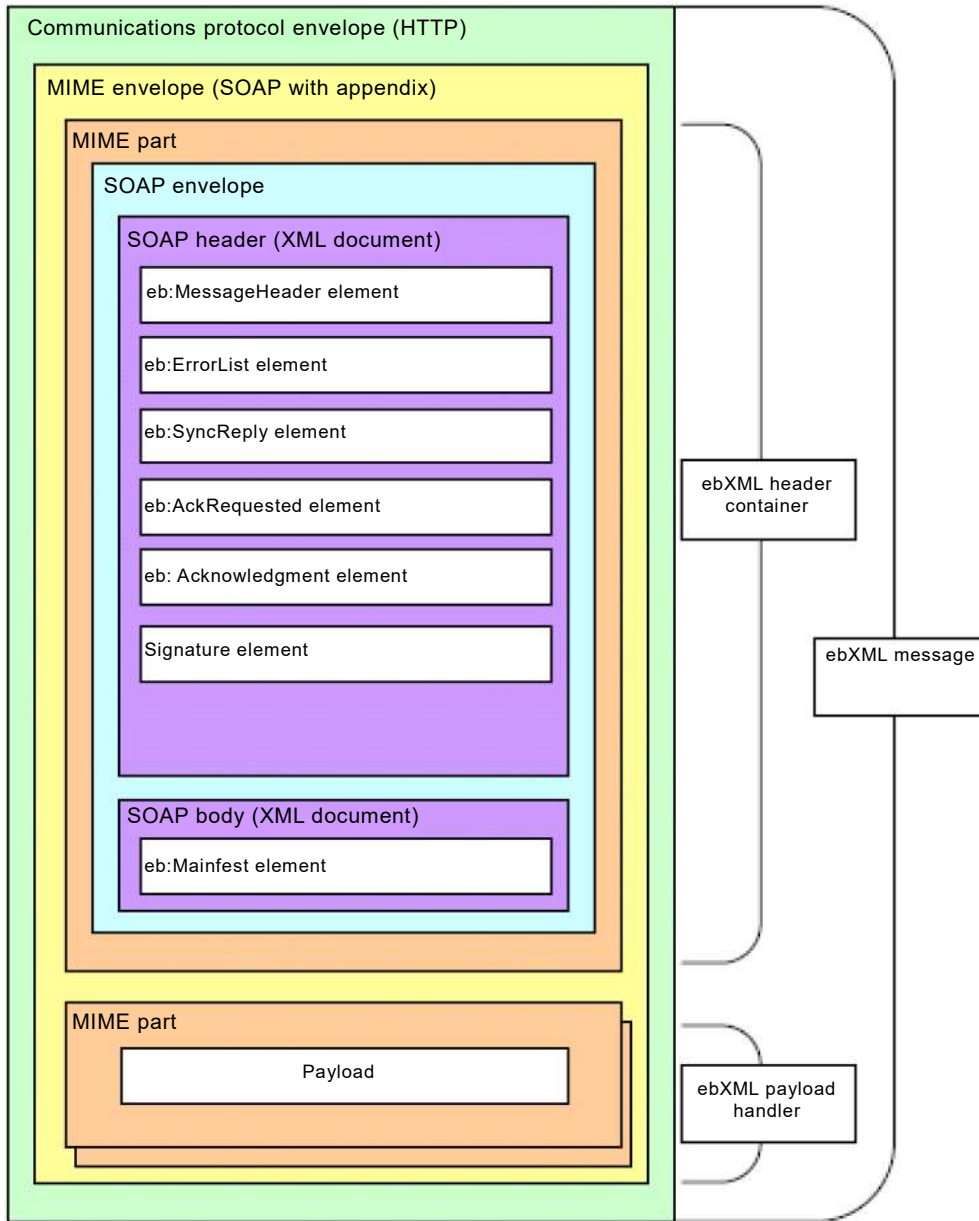
Figure 4.5.3 shows ebMS2.0 message format.

Figure 4.5.3 ebMS2.0 message format

4.5.4　Setting for ebMS processing mode

(1)　Message type
　　Table 4.5.2 shows message types used in ebMS processing mode, necessity of digital signature and Acknowledgment /ErrorList.

Table 4.5.2 Message types used in ebMS processing mode

Message Type	Digital signature	Acknowledgment/ErrorList
Procedure message NACCS EDI message	Necessary	Necessary
Procedure message XML format message	Necessary	Necessary
Processing Result Message	Necessary	Necessary
Acknowledgment	Necessary	Unnecessary
Errorlist	Unnecessary	Unnecessary

(2)　Service/Action element
　　Communication conditions (Message Type) which are according to CPA are specified by defining Service elements and Action elements. In actual transactions, both elements are written in SOAP header in the following manner.

```
<eb:Service eb:type="XXX">XXXXX</eb:Service>
<eb:Action>XXXXX</eb:Action>
```

　　When Service and Action are specified, each element in DeliveryChannel, Packaging, Transport, and DocExchange, which are according to CPA, will be uniquely determined and communication conditions will be identified based on those details.
　(For details of each element, refer to "4.5.4 (3) Setting of CPA")

　　Table 4.5.3 shows Service elements and Action elements used in ebMS processing mode.

Table 4.5.3 Service/Action Used in ebMS Processing Mode

Message Type	Service	Action
Procedure message NACCS EDI message	urn:NACCS:ICS:BusinessService	NACCS-EDI
Procedure message XML format message	urn:NACCS:ICS:BusinessService	NACCS-XML
Processing Result Message	urn:NACCS:ICS:BusinessService	NACCS-Result
Processing Result Request Message	urn:NACCS:ICS:BusinessService	NACCS-ResultReq
Acknowledgment	urn:oasis:names:tc:ebxml-msg:service	Acknowledgment
Errorlist	urn:oasis:names:tc:ebxml-msg:service	MessageError

(3) Setting of CPA
Table 4.5.4 shows an example of setting of CPA used in ebMS processing mode.

Table 4.5.4 Setting of CPA Specified in ebMS Processing Mode (Example)

Item to be set	Details of setting	Setting value
Cpaid	CPA ID used for communication	designated by NACCS Center
PartyInfo	Information of each transactor	
partyName	Name of transactor (Unique in CPA)	designated by NACCS Center
PartyId	Transactor's identification ID (Unique in CPA)	designated by NACCS Center
CollaborationRole	Setting for messages used in transactions	
ServiceBinding	Linking between services and communication conditions	
Service	Name of service	See Table 4.5.3.
CanSend CanReceive	Attribute of Action (e.g.) For communications of Party 1 and Party 2, when attribute of Action 1 is specified as CanSend for Party 1 and CanRecieve for Party 2, in communication of Action 1, Party 1 becomes transmission side and Party 2 becomes receipt side.	Specified for each action.
This Party Action Binding	Linking between actions and communication conditions	
Action	Name of action	See Table 4.5.3.
Business Transaction Characteristics	Transaction characteristics	
is NonRepudiation Required	Whether using XML signature when parent element of action is used ?	true
isNonRepudiationReceiptRequired	Whether adding XML signature to acknowledgment of receipt (Acknowledgment) ?	true
is Confidential	Whether encrypting messages ?	transient
is Authenticated	Whether adding XML signature to identify sender ?	transient
is Authorization Required	Is authentication of sender necessary?	true
Delivery Channel	Linking between actions and Transport / DocExchange	
Messaging Characteristics	Characteristics in exchange of messages	

Item to be set	Details of setting	Setting value
sync ReplyMode	Whether requesting synchronous mode response ?	none
ackRequested	Whether requesting acknowledgment of receipt ?	always
ackSignature Requested	Whether adding XML signature to acknowledgment of receipt ?	always
duplicate Elimination	Whether carrying out duplication of messages ?	always
Transport	Communications protocol and destination URL	
Transport Protocol	Name of communications protocol	HTTP
Version	Version information	1.1
Transport Client Security	Security during forwarding	
Transport Security Protocol	Name of security protocol for transport layer	TLS
Version	Version information	1.2
DocExchange	Conditions for exchange of messages (When there are multiple Actions in one CPA seen this system, DocExchange is specified for each conditions for exchange)	
ebXMLSenderBinding ebXMLReceiverBinding	Setting for sender and receiver Both DocExchanges directly corresponding as sender / receiver of Action should have the same setting)	
version	Version information	2.0
ReliableMessaging	Function to guarantee messages	
Retries	Number of retry	3 (standard value)
RetryInterval	Interval of retry	PT10M (standard value: every 10 minutes)
MessageOrderSemantics	Whether carrying out guarantee of message order ?	NotGuaranteed
PersistDuration	Retention period for messages	PT1H (standard value: 1 hour)

4.5.5 Message format and structure

When using ebMS processing mode, NACCS EDI messages and XML format messages which store necessary information for procedures are stored in payload section. In addition, communications protocol (HTTP) header, SOAP header, SOAP body, and communications protocol (HTTP) trailer are added.

The message formats are outlined as follows:

(1) XML format message
   Figure 4.5.4 shows outline of XML format messages (ebMS processing mode).

XML Format Message

| Communications protocol header (HTTP Header) | SOAP header | SOAP body | XML message | Communications protocol trailer (HTTP header) |

Max. 700,000 bytes (Note)
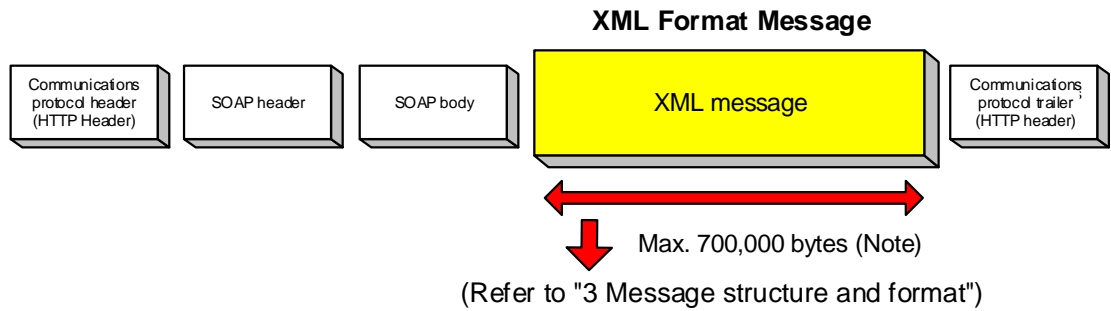(Refer to "3 Message structure and format")

Figure 4.5.4 Outline of XML Format Message (ebMS Processing Mode)

For procedure subjected to XML format messages, refer to "Appendix Table 6.7 Subjected Procedure List." In addition, message format / version are according to PAA (Pan Asian e-commerce Alliance) Standard/Superset Message Structure V2.0).

(2) NACCS EDI message

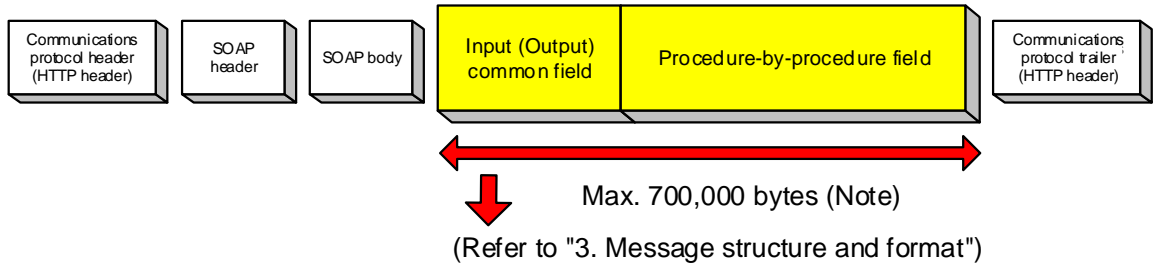Figure 4.5.5 shows outline of the NACCS EDI message format (ebMS processing mode).

Figure 4.5.5 Outline of NACCS EDI Message Format (ebMS Processing Mode)

Figure 4.5.6 shows the format of a message created when user of ebMS processing mode send a NACCS EDI message to the NACCS Center server.

NACCS EDI Message											
Input (Output) common field			Procedure-by-procedure field								
…	CR	LF	…	CR	LF	…	CR	LF	…	CR	LF

Figure 4.5.6 Message Segmentation

4.5.6　Procedure sequential processing

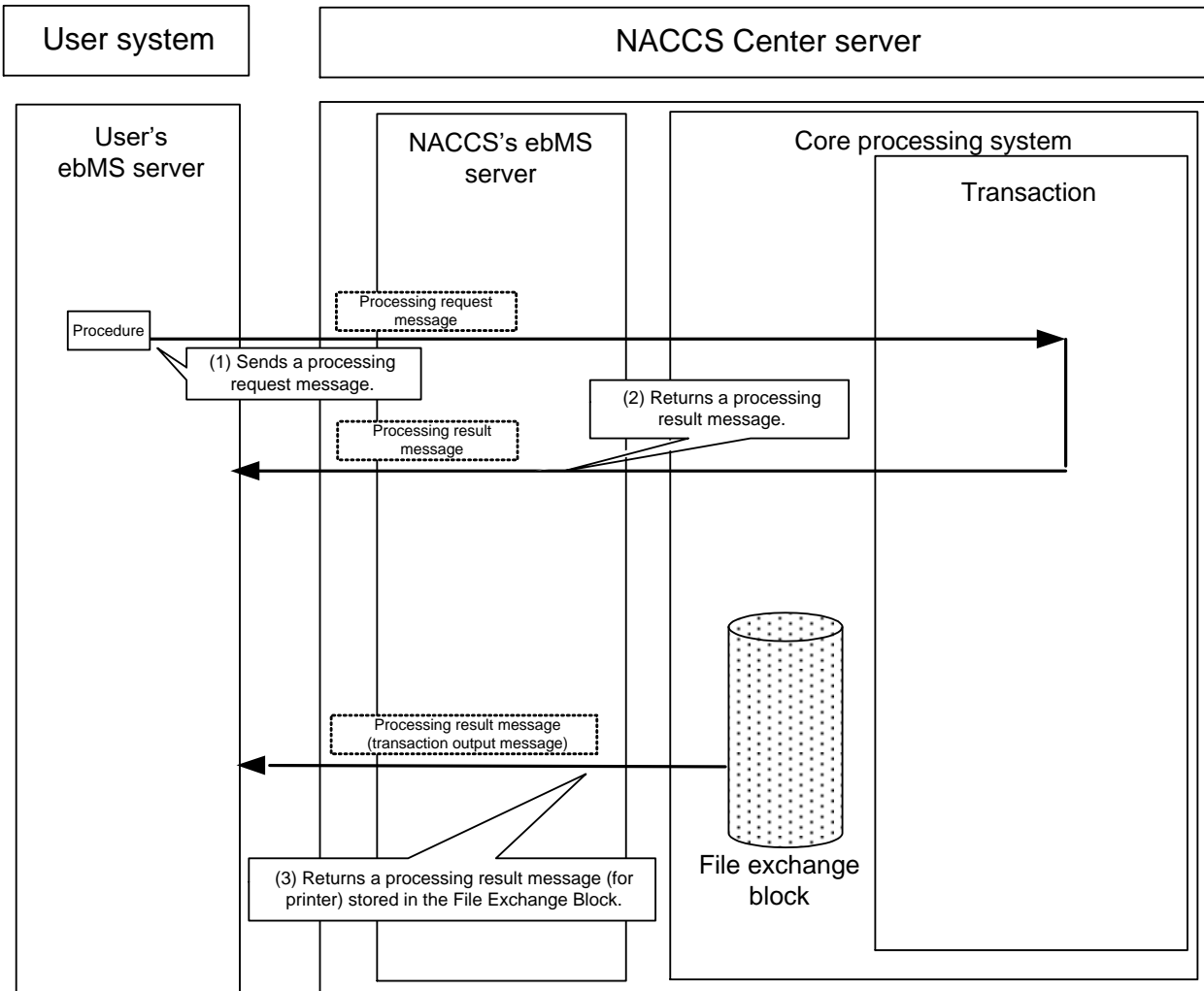Figure 4.5.7 shows procedure processing sequence in ebMS processing mode.

Figure 4.5.7 Example of Procedure Processing Sequence in ebMS Processing Mode

(1) User sends a processing request message where necessary fields for the procedure are input to the NACCS Center server.
(2) A processing result message is returned from the NACCS Center server to the user system.
(3) When there is a transaction output message, the transaction output message will be returned from the NACCS Center server to the user system.

In addition, when using multiple payload function, user receives processing result messages and transaction output messages of the equivalent amount of procedures incorporated in Payload section from the NACCS Center server in response to one processing request message (where multiple procedure messages are included in Payload section).