3G-Web Development Guide

Ver. 1.4.10β (June 2016~)

Table of Contents

Chapter 1 Getting Started with 3G-Web 3
1-1 Contents of this Guide 3
1-2 Intended Audience 3
1-3 Limitations 3
1-4 Copyright and Contact Details 4
1-5 Revision History 4

Chapter 2 Overview of 3G-Web 5
2-1 Payment Services Available in 3G-Web 5
2-2 About Sample Programs 5
2-3 Sample Program Process Overview 6
2-4 Process Overview of Available Services in 3G-Web 9
2.4.1 Credit Card Payment 9
2.4.2 Credit Card Payment (with 3-D Secure) 10
2.4.3 Convenience Store Payment 10
2.4.4 E-Money Payment 12
2.4.5 Bank Payment 15

Chapter 3 Handling Result Notification 18
3-1 Target of Result Notification Process 18
3.1.1 Result Notification Process from 3G-Web 18
3.1.2 Result Notification Process from VeriTrans3G 18

Chapter 4 Interface Details 20
4-1 Access URL 20
4-2 Encryption Key Acquisition 20
4-3 3G-Web Redirect 26
4-4 Payment Result Verification 26
4-5 Result Notification Message from 3G-Web 27
4.5.1 Overview of Result Notification Message 27
4.5.2 Result Notification 28
4-6 Result Notification Message from VeriTrans3G 29

Chapter 5 Other - Supplementary Items 30
5-1 Notes for Testing 30
5-2 Verification of Test Transaction Results on MAP 31

Chapter 1 Getting Started with 3G-Web

1-1 Contents of this Guide

This guide contains information about sample programs and message formats, which can be used as reference when connecting from merchant's EC site to 3G-Web offered by VeriTrans Inc.

1-2 Intended Audience

This is intended for the developers of merchants' EC site, which connects to 3G-Web.

Title	Overview	Planner	Developer	Operator
3G-Web Development Guide	Provides information about how to connect to 3G-Web from merchant's EC site.		◎	

Table 1-2-1 List of Documents

1-3 Limitations

There are following limitations when connecting to 3G-Web from merchant's EC site.

[Consumer environment]

Consumer can use it in the following environments (browsers).

(Depending on the environment, it may not work properly.)

■ PC

- Internet Explorer 11 or above
- Microsoft Edge latest stable version
- Google Chrome latest stable version
- Mozilla Firefox latest stable version
- Safari latest stable version

■ Smartphone

- Standard browser

■ Feature phone

- Mobile phones having SHA-2 certificate such as i mode (docomo), EZweb (au), Yahoo! Mobile (SoftBank) and the conventional mobile phones, which support SSL/TLS communication

  Note) When supporting the terminal, which does not support communication with TLS1.1 or above, please refer to the 4-1 and take an appropriate action.

[JavaScript]

3G-Web uses the JavaScript to redirect the page. So, if the consumer is using PC or smartphone, 3G-Web cannot be used on the Web browser where JavaScript is turned OFF.

If the consumer is using feature phone, 3G-Web displays only the pages, where JavaScript is not used.

[Other]

For Other constraints, please check the 3G-Web integration document.

1-4 Copyright and Contact Details

[Contact Details] Technical Support, VeriTrans Inc. E-mail: tech-support@veritrans.jp

1-5 Revision History

Chapter 2 Overview of 3G-Web

2-1 Payment Services Available in 3G-Web

The following online payment services can be used by merchants by connecting to our 3G-web by customizing and integrating the provided sample programs to their own EC site.

Payment Service Name	Description
Credit card	This is a payment service using credit cards. This service enables making payments with credit cards issued by various brands and card companies. *1
Credit card (With 3-D Secure)	This service enables credit card payment with 3-D Secure function. Our 3-D Secure function supports 3 international card brands VISA/MASTER/JCB. ∗ Feature phone does not support 3-D Secure. When accessing through feature phone, it becomes a regular credit card payment.
Convenience store	This service enables making payments through convenience store such as 7-Eleven, LAWSON, FamilyMart, Circle K Sunkus etc.
E-Money	This service enables making payments through electronic money payment service such as Rakuten Edy, Suica, WAON etc.
Bank	This service enables making payments through financial institutions such as bank. Payments can be made through ATM (Pay-easy) and Internet banking.

Table 2-1-1 List of Payment Services

∗1: Only one merchant account number specified by Acquirer can be assigned to one merchant ID held by merchant.

2-2 About Sample Programs

In 3G-Web, we offer a functional set as a sample program, for EC sites from which merchants connect to 3G-Web.

Merchants can use the sample programs by customizing it. They can even customize the pages as per their EC site's requirements. (Please note that customization is to be done at the merchant's end).

We provide sample programs for multiple languages such as Java, PHP etc.

The merchant can carry out a payment through a contractual 3G-Web service. The merchant can then use multiple 3G-Web services simultaneously.

Please refer to the separate "Installation Guide" for installation of sample programs as per the language.

2-3 Sample Program Process Overview

The following figure shows the operation of sample programs.

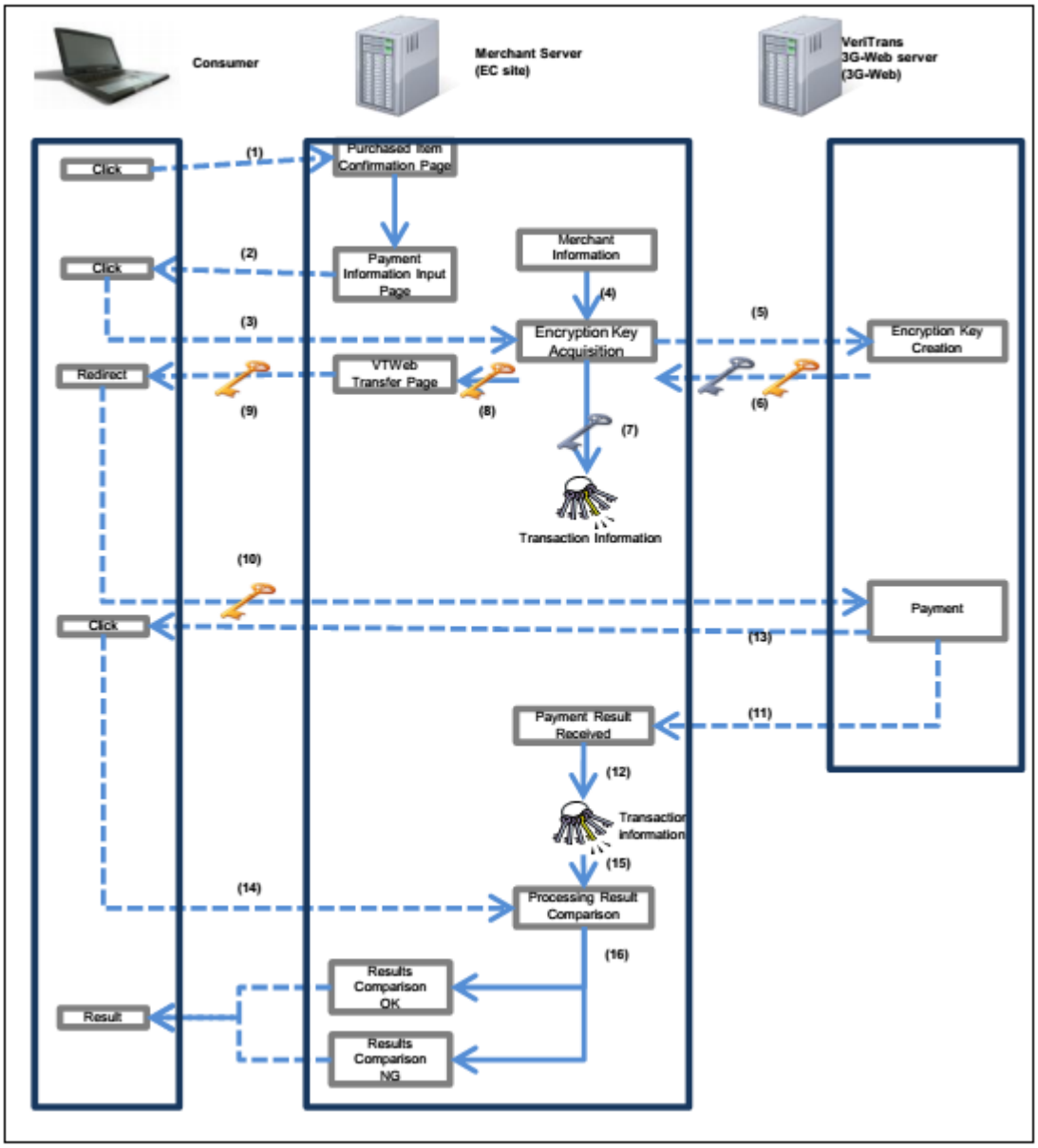

Figure 2-3-1 Sample Program Overview

"Figure 2-3-1 Sample Program " is explained below in detail. Please check it against the numbers in Figure.

(1) This 'Purchased Item Confirmation Page' is assumed to be a page for final confirmation before actual payment.

(2) When the consumer clicks the "Purchase" button in process (1), it redirects to 'Payment Information Input Page'.

(3) When the consumer selects the payment type (mode of payment) and input the personal information in the 'Payment Information Input Page', it moves to the following process of 'Encryption Key Acquisition'.

∗ Here, before integration the merchant will decide whether he wants the consumer to input the information such as payment type or his personal information and merchant will inform that decision to VeriTrans.

(4) In 'Encryption Key Acquisition', information like merchant ID, return URL after payment etc. as described in the setup file, is acquired.

∗ Please refer to the [Installation Guide] for the items defined in setup file.

∗ Also at this stage, the Order ID will be assigned at EC site.

(5) The EC site requests Encryption Key Acquisition to 3G-Web. For transmission/ reception parameters, please refer to "Chapter 4 Interface Details".

(6) In return, the EC site receives an encryption key for the consumer (hereinafter, browser encryption key) and encryption key for the EC site (hereinafter, merchant encryption key) from 3G-Web. For transmission/reception parameters, please refer to "Chapter 4 Interface Details".

(7) EC site stores the order ID as a key and stores merchant encryption key in transaction information. For the items to be stored in transaction information, please refer to the "Chapter 4 Interface Details".

∗ In the sample program, to make it simple and easy to understand, it is saved as a HashMap (Java) or text file (PHP), but it is recommended to save it in the Database.

(8) The received information is passed to the 3G-Web redirect page.

(9) The consumer browser will be redirected to the 3G-Web Redirect page. For request/response parameters, please refer to the "Chapter 4 Interface Details".

(10) The consumer browser will be redirected from the 3G-Web Redirect page to the 3G-Web. Here all the parameters that are passed in step (8) will be passed to 3G-Web.

After redirection, the consumer will input the required information in the 3G-Web to make a payment.

(11) After payment completion, 3G-Web notifies the payment result to the EC site. For request/response parameters, please refer to the "Chapter 4 Interface Details".

(12) The EC site assumes the order ID of received payment results as a key, and gets the information of corresponding transactions from transaction information and stores the received payment result information.

∗ To make the figure easy to understand, it is described separately, but the 'Transaction Information' here and in step (7) is the same.

(13) 3G-Web returns the payment result to the consumer browser. The payment result information is returned here and the information returned in step (11) is the same. This information will be used for the comparison in step (15).

(14) The consumer browser will be redirected to the return URL of the EC site. This return URL is the URL, which was sent to 3G-Web in step (5). At this time all the parameters, which were passed from 3G-Web in step (13) are passed as it is. For request/response parameters, please refer to the "Chapter 4 Interface Details".

(15) The EC site performs a process result comparison. In this comparison, considering the order ID as a key, information of the corresponding transaction is acquired from the transaction information and the passed parameters are verified.

(16) As a result of 'Process Result Comparison', if there is no issue, then 'Result Comparison success, and if there is an issue,

then ’Result Comparison failure is returned to the consumer browser.

* In sample programs only the process results are compared. But in actual operation, the merchant can carry out a ’Bifurcation based on the value of process result or error code’ whenever necessary.

2-4 Process Overview of Available Services in 3G-Web

This section explains the process overview (process flow) for each payment service.

The light blue color frame in the following figure shows the below-mentioned VeriTrans servers.

Web: 3G-Web Server

Payment Gateway: VeriTrans 3G Server

2.4.1 Credit Card Payment

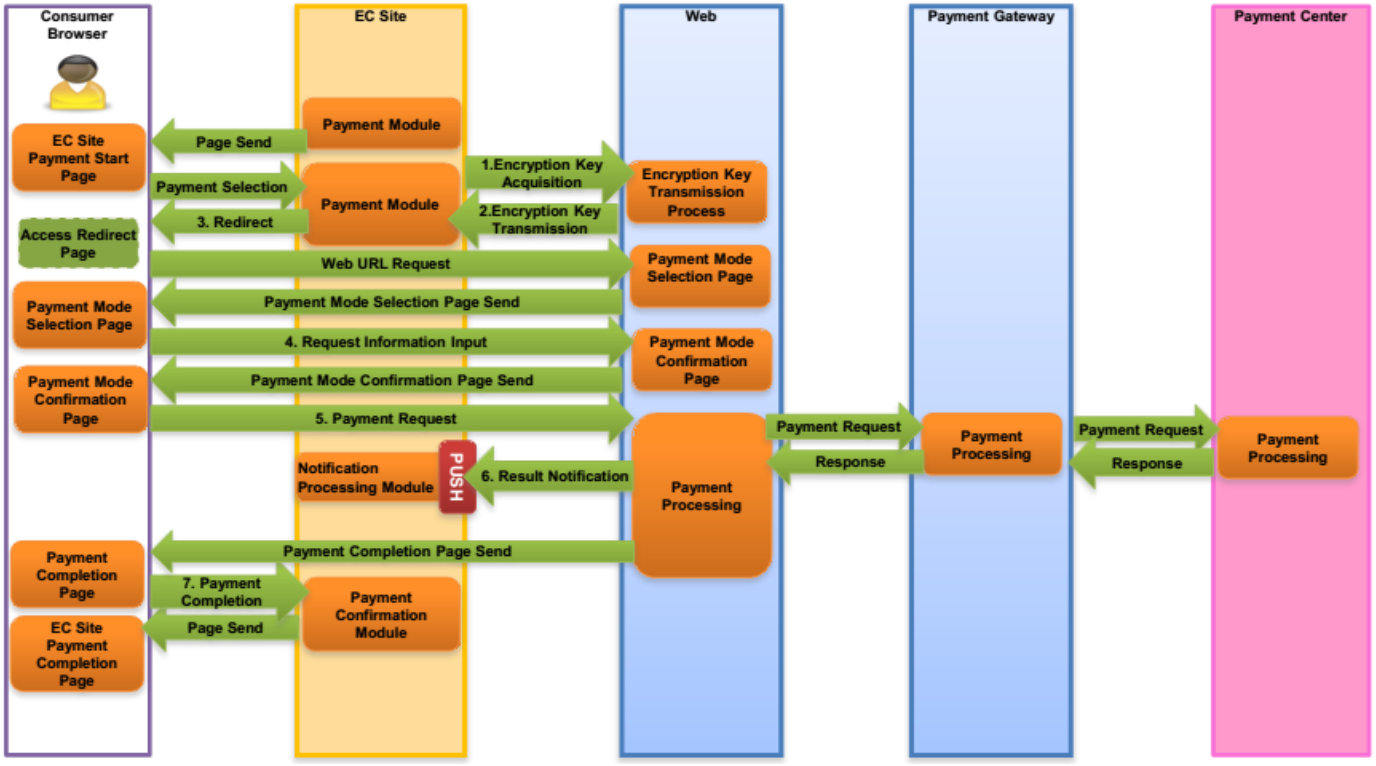

Figure 2-4-1 System Process Overview Diagram when Using 3G-Web (Credit Card Payment)

No.	Basic Functions	Description
1	Encryption Key Acquisition	Sends payment request received from request module of EC site to 3G-Web.
2	Encryption Key Transmission	3G-Web receives a request from EC site, creates an encryption key for consumer (Hereinafter, browser encryption key) and for EC site respectively and returns it to EC site.
3	Redirect	EC site sends order ID, browser encryption key and URL of 3G-Web to consumer, and prompts the consumer to redirect to 3G-Web Payment Page. ∗ When displaying the 3G-Web payment page, instead of displaying the pop-up on a different page, display it on the same page.
4	Payment Information Input	Consumer selects the Payment type and inputs the required information. After selecting payment type, consumer browser redirects to the payment confirmation page.
5	Payment Request	Consumer makes payment request.
6	Result Notification	3G-Web sends the Result notification to EC site in POST format.
7	Payment Completion	When consumer clicks the button “Return to EC site”, 3G-Web redirects to EC site’s payment completion page.

Table 2-4-1 3G-Web Integration Process Overview (Credit Card Payment)

2.4.2 Credit Card Payment (with 3-D Secure)

* Feature phone does not support 3-D Secure.

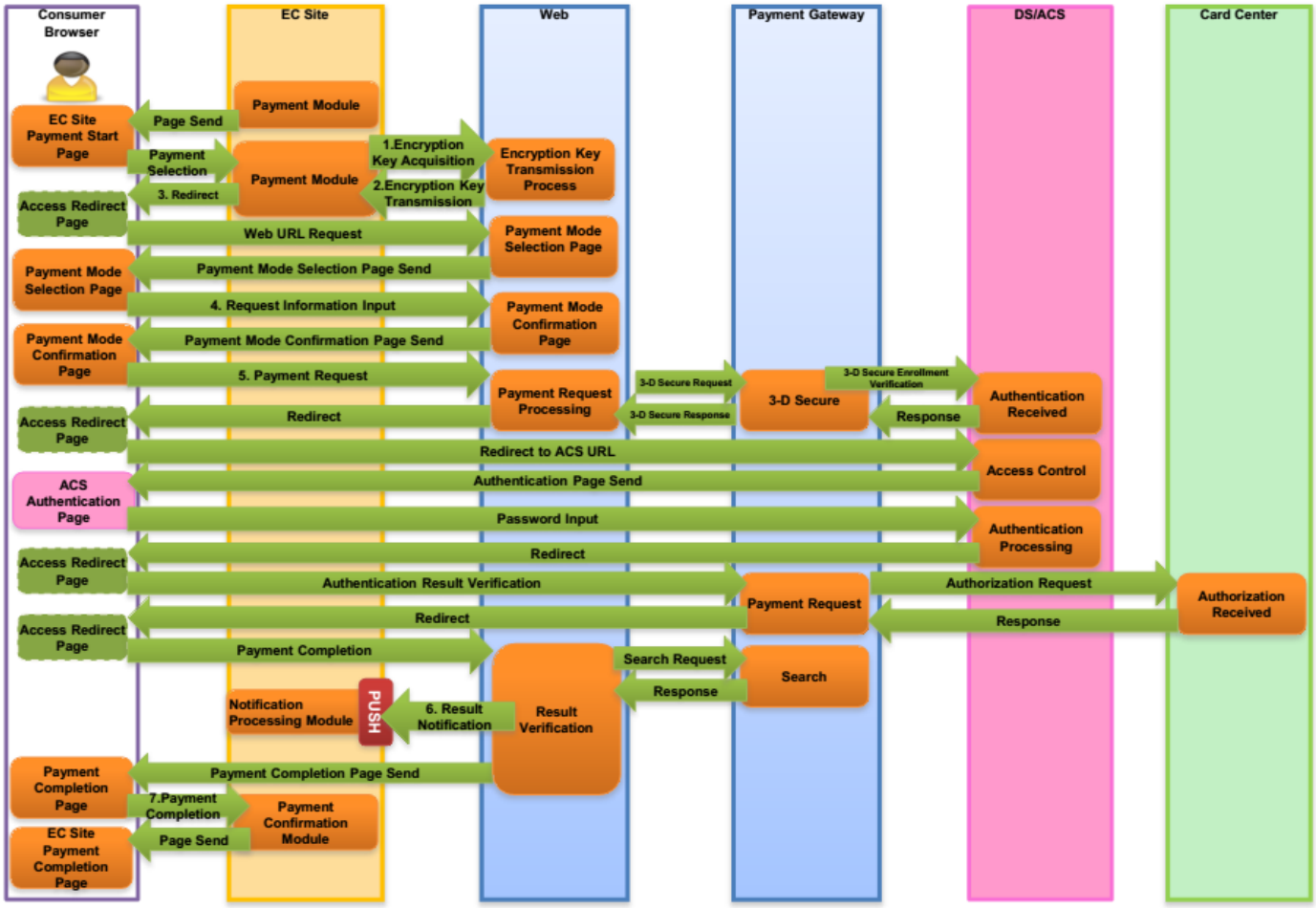

Figure 2-4-2 System Process Overview Diagram when Using 3G-Web (Credit Card Payment (with 3-D Secure)

No.	Basic Functions	Description
1	Encryption Key Acquisition	Sends payment request received from request module of EC site to 3G-Web.
2	Encryption Key Transmission	3G-Web receives a request from EC site, creates an encryption key for consumer (Hereinafter, browser encryption key) and for EC site respectively and returns it to EC site.
3	Redirect	EC site sends order ID, browser encryption key and URL of 3G-Web to consumer, and prompts the consumer to redirect to 3G-Web Payment Page. ∗ When displaying the 3G-Web payment page, instead of displaying the pop-up on a different page, display it on the same page.
4	Payment Information Input	Consumer selects the Payment type and inputs the required information. After selecting payment type, consumer browser redirects to the payment confirmation page.
5	Payment Request	Consumer makes the payment request. When 3-D Secure is enabled, consumer browser redirects to the ACS authorization page. When 3-D Secure is disabled, it redirects to error page.
6	Result Notification	3G-Web sends the Result notification to EC site in POST format.
7	Payment Completion	When consumer clicks the button “Return to EC site”, 3G-Web redirects to EC site’s payment completion page.

Table 2-4-2 3G-Web Integration Process Overview (Credit Card Payment (with 3-D Secure))

2.4.3 Convenience Store Payment

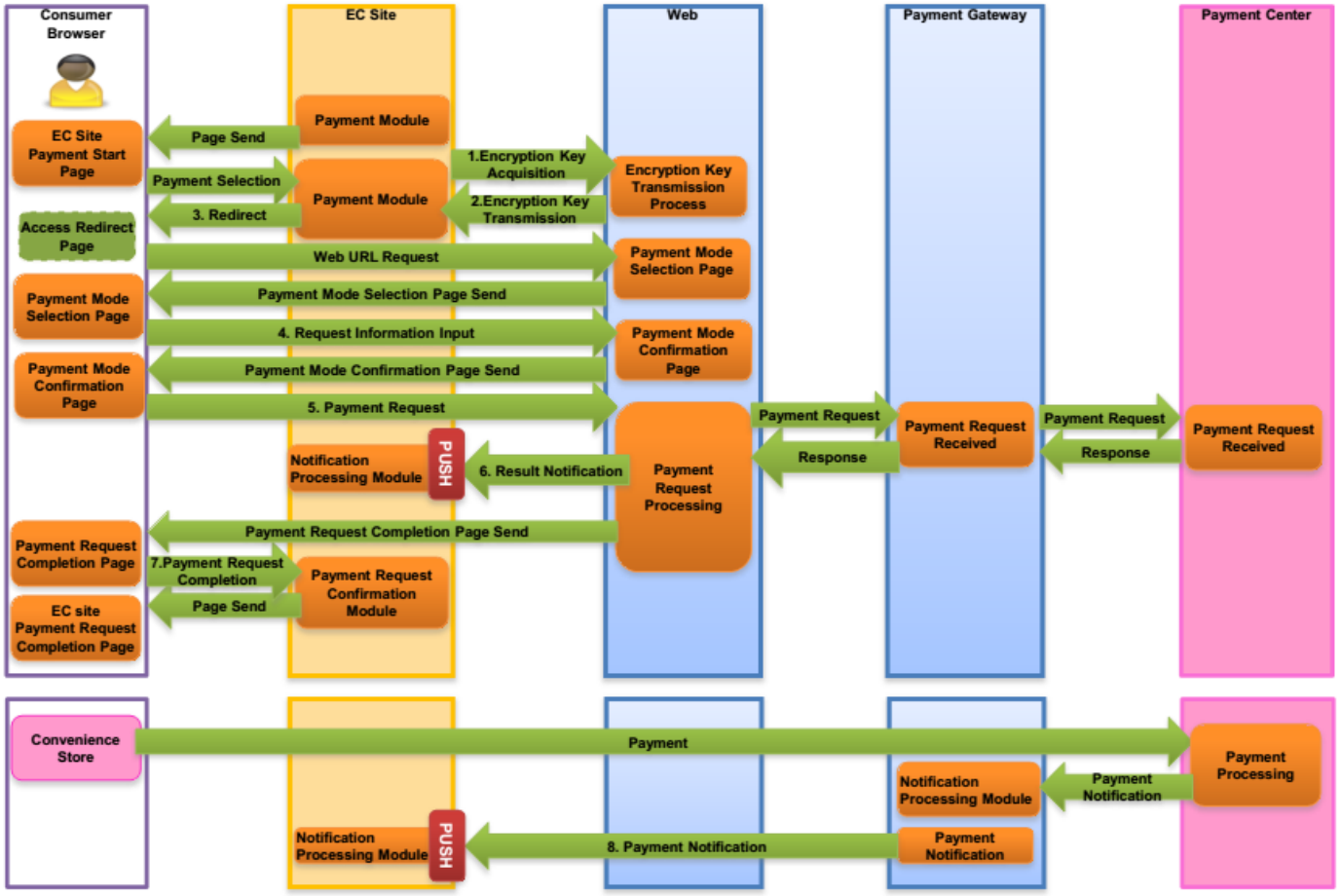

Figure 2-4-3 System Process Overview Diagram when Using 3G-Web (Convenience Store Payment)

No.	Basic Functions	Description
1	Encryption Key Acquisition	Sends payment request received from request module of EC site to 3G-Web.
2	Encryption Key Transmission	3G-Web receives a request from EC site, creates an encryption key for consumer (Hereinafter, browser encryption key) and for EC site respectively and returns it to EC site.
3	Redirect	EC site sends order ID, browser encryption key and URL of 3G-Web to consumer, and prompts the consumer to redirect to 3G-Web Payment Page. ∗ When displaying the 3G-Web payment page, instead of displaying the pop-up on a different page, display it on the same page.
4	Payment Information Input	Consumer selects the Payment type and inputs the required information. After selecting payment type, consumer browser redirects to the payment confirmation page.
5	Payment Request	Consumer makes payment request.
6	Result Notification	3G-Web sends the Result notification to EC site in POST format.
7	Payment Completion	When consumer clicks the button “Return to EC site”, 3G-Web redirects to EC site’s Payment Completion Page.
8	Payment Notification	Notifies payment notification to EC site once VeriTrans3G verifies the payment has been received from the consumer, for that particular transaction. The notification is sent in POST format.

Table 2-4-3 3G-Web Integration Process Overview (Convenience Store Payment)

2.4.4 E-Money Payment

[E-Money Payment (PC Edy/PC Suica/PC WAON)]

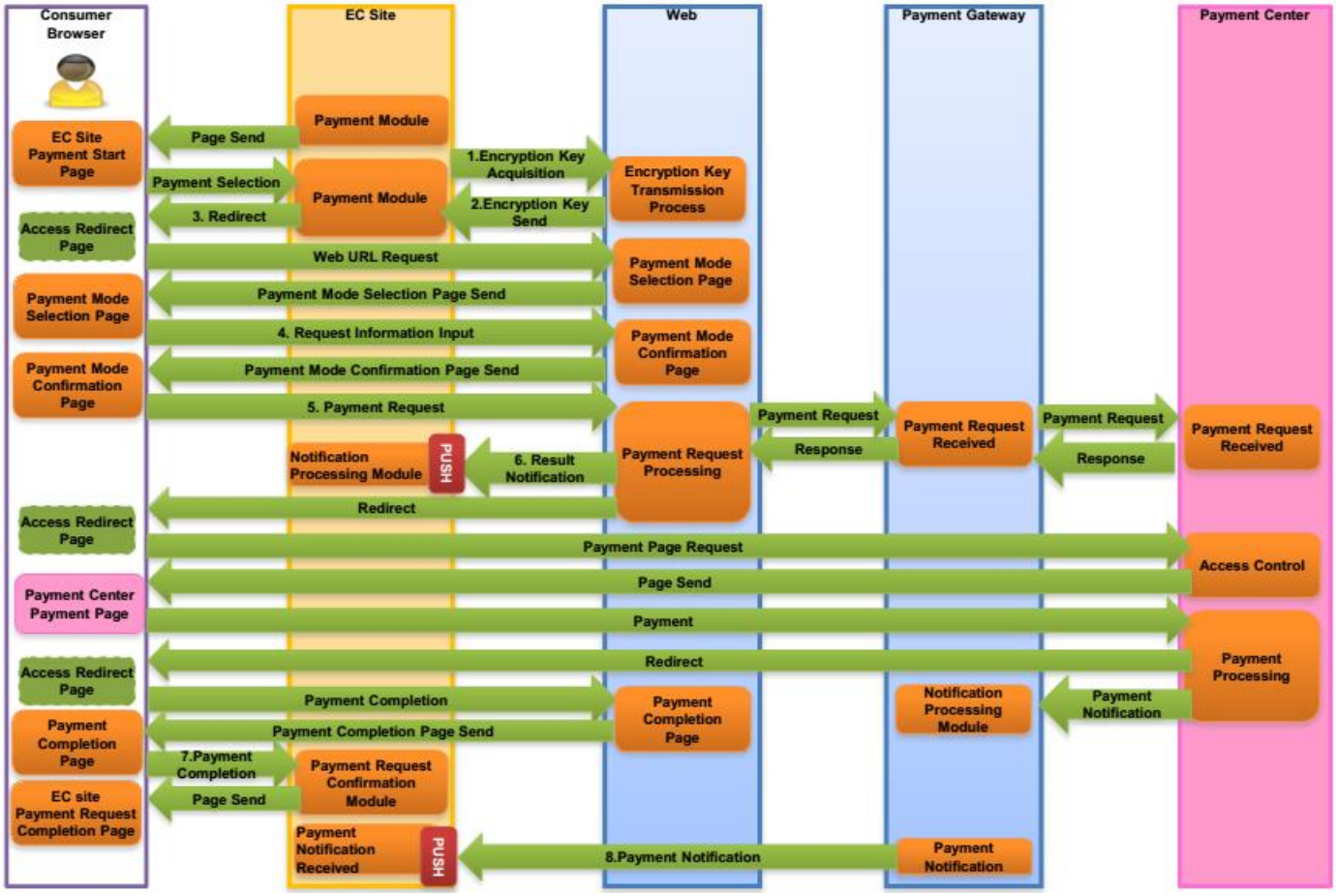

Figure 2-4-4 System Process Overview Diagram when Using 3G-Web (E-Money Payment (PC Edy/PC Suica/PC WAON))

No.	Basic Functions	Description
1	Encryption Key Acquisition	Sends payment request received from request module of EC site to 3G-Web.
2	Encryption Key Transmission	3G-Web receives a request from EC site, creates an encryption key for consumer (Hereinafter, browser encryption key) and for EC site respectively and returns it to EC site.
3	Redirect	EC site sends order ID, browser encryption key and URL of 3G-Web to consumer, and prompts the consumer to redirect to 3G-Web payment page. ∗ When displaying the 3G-Web payment page, instead of displaying the pop-up on a different page, display it on the same page.
4	Payment Information Input	Consumer selects the Payment type and inputs the required information. After selecting payment type, consumer browser redirects to the payment confirmation page.
5	Payment Request	Consumer makes payment request. When consumer makes payment request, consumer browser will redirect to payment page of payment center.
6	Result Notification	3G-Web sends the result notification to EC site in POST format.
7	Payment Completion	When consumer clicks the button “Return to EC site”, 3G-Web redirects to EC site’s payment completion page.
8	Payment Notification	Notifies payment notification to EC site once VeriTrans3G verifies the payment has been received from the consumer, for that particular transaction. The notification is sent in POST format.

Table 2-4-4 3G-Web Integration Process Overview (E-Money Payment (PC Edy/PC Suica/PC WAON))

[E-Money Payment (Mobile Edy/Mobile Suica)]

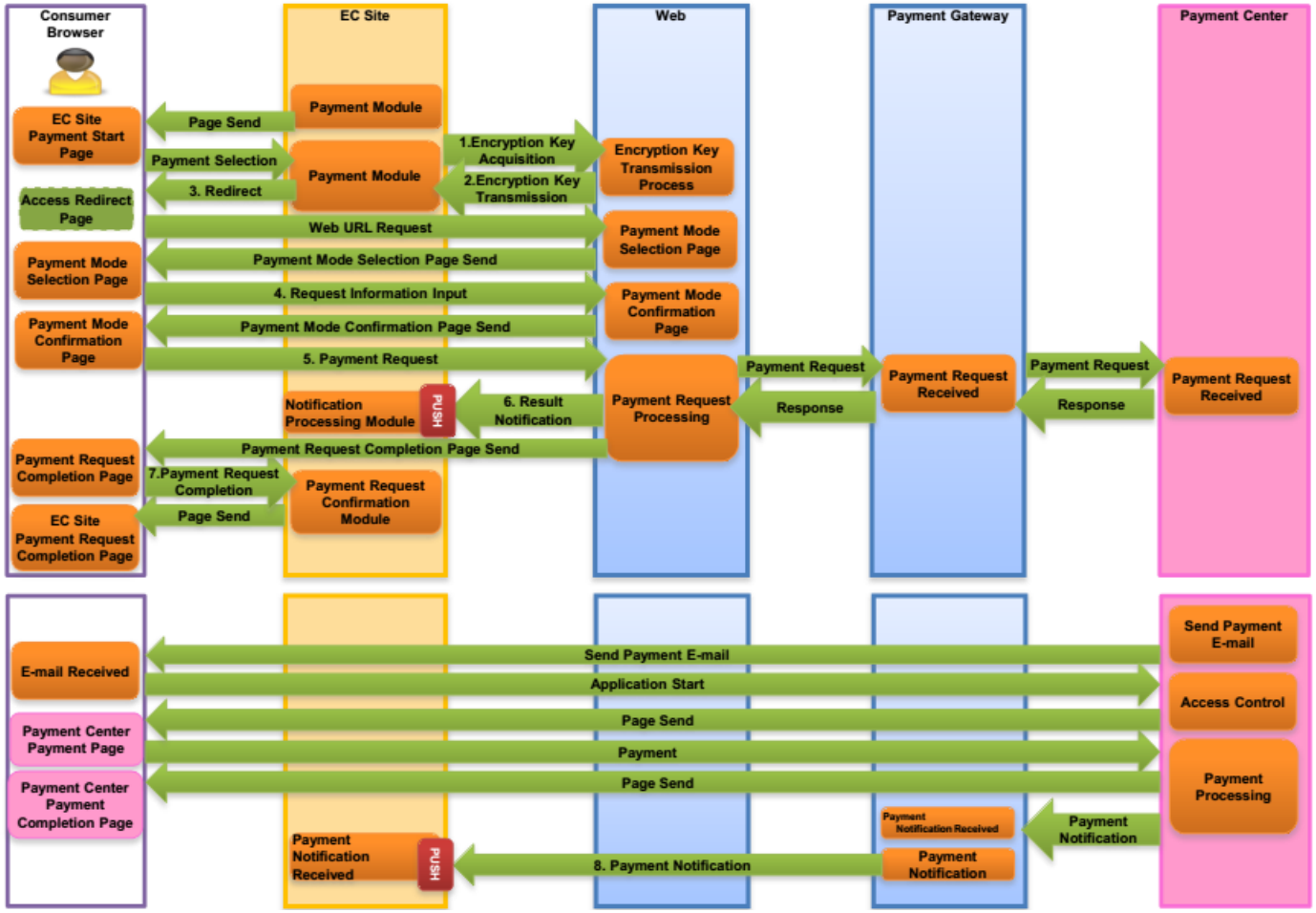

Figure 2-4-5 System Process Overview Diagram when Using 3G-Web (E-Money Payment (Mobile Edy/Mobile Suica))

No.	Basic Functions	Description
1	Encryption Key Acquisition	Sends payment request received from request module of EC site to 3G-Web.
2	Encryption Key Transmission	3G-Web receives a request from EC site, creates an encryption key for consumer (Hereinafter, browser encryption key) and for EC site respectively and returns it to EC site.
3	Redirect	EC site sends order ID, browser encryption key and URL of 3G-Web to consumer, and prompts the consumer to redirect to 3G-Web payment page. ∗ When displaying the 3G-Web payment page, instead of displaying the pop-up on a different page, display it on the same page.
4	Payment Information Input	Consumer selects the Payment type and inputs the request information. After selecting payment type, consumer browser redirects to the payment confirmation page.
5	Payment Request	Consumer makes payment request.
6	Result Notification	3G-Web sends the result notification to EC site in POST format.
7	Payment Completion	When consumer clicks the button “Return to EC site”, 3G-Web redirects to EC site’s payment completion page.
8	Payment Notification	Notifies payment notification to EC site once VeriTrans3G verifies the payment has been received from the consumer, for that particular transaction. The notification is sent in POST format.

Table 2-4-5 3G-Web Integration Process Overview (E-Money Payment (Mobile Edy/Mobile Suica))

[E-Money Payment (Mobile WAON)]

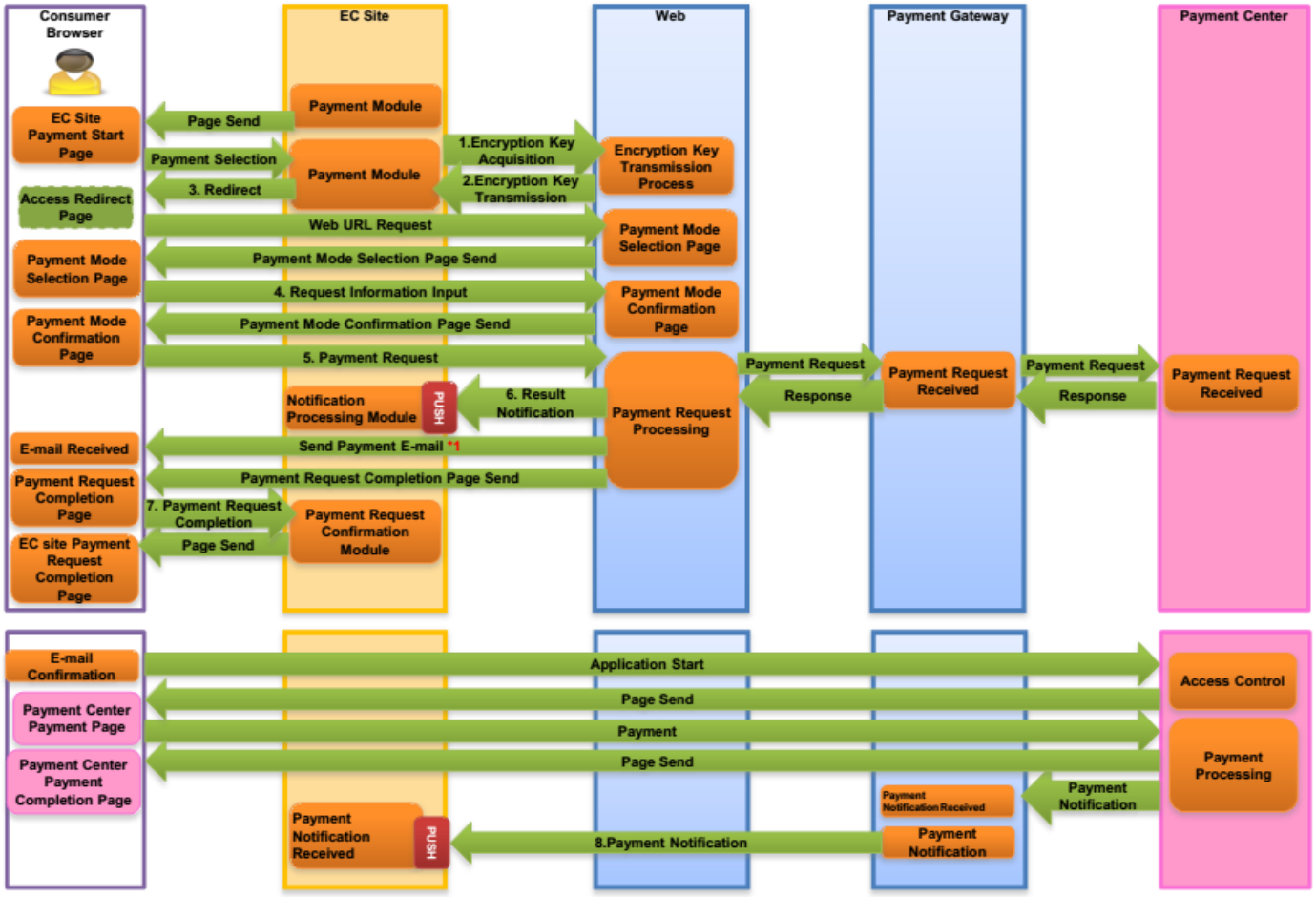

Figure 2-4-6 System Process Overview Diagram when Using 3G-Web (E-Money Payment (Mobile WAON))

No.	Basic Functions	Description
1	Encryption Key Acquisition	Sends payment request received from request module of EC site to 3G-Web.
2	Encryption Key Transmission	3G-Web receives a request from EC site, creates an encryption key for consumer (Hereinafter, browser encryption key) and for EC site respectively and returns it to EC site.
3	Redirect	EC site sends order ID, browser encryption key and URL of 3G-Web to consumer, and prompts the consumer to redirect to 3G-Web payment page. ∗ When displaying the 3G-Web payment page, instead of displaying the pop-up on a different page, display it on the same page.
4	Payment Information Input	Consumer selects the Payment type and inputs the request information. After selecting payment type, consumer browser redirects to the payment confirmation page.
5	Payment Request	Consumer makes payment request.
6	Result Notification	3G-Web sends the result notification to EC site in POST format.
7	Payment Completion	When consumer clicks the button “Return to EC site”, 3G-Web redirects to EC site’s payment completion Page.
8	Payment Notification	Notifies payment notification to EC site once VeriTrans3G verifies the payment has been received from the consumer, for that particular transaction. The notification is sent in POST format.

Table 2-4-6 3G-Web Integration Process Overview (E-Money Payment (Mobile WAON))

*1: In WAON payment, payment E-mail is sent from 3G-Web to consumer. (In other E-Money payment, payment E-mail is sent directly to consumer from respective payment company.)

2.4.5 Bank Payment

[Bank Payment (ATM)]

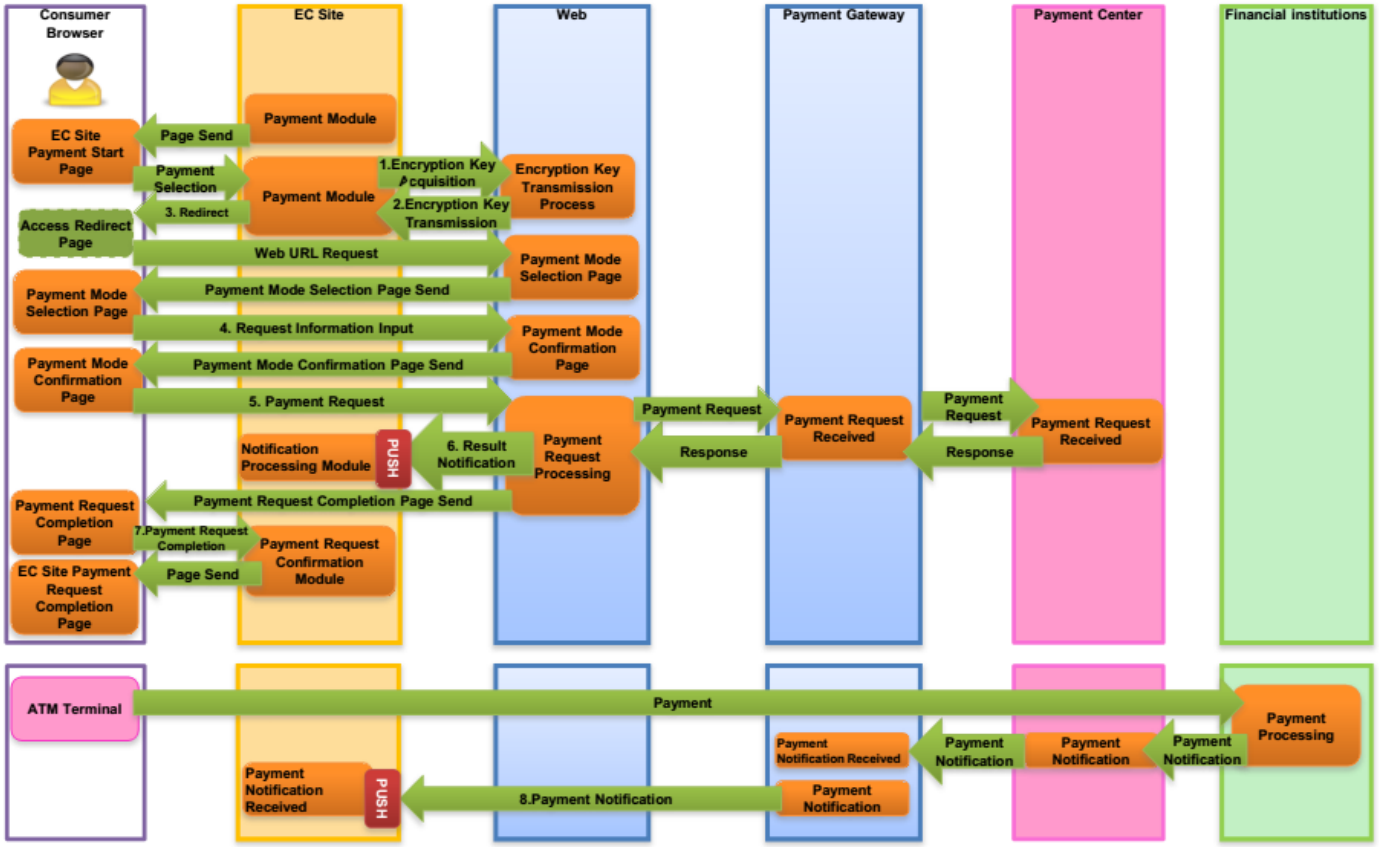

Figure 2-4-7 System Process Overview Diagram when Using 3G-Web (Bank Payment (ATM))

No.	Basic Functions	Description
1	Encryption Key Acquisition	Sends payment request received from request module of EC site to 3G-Web.
2	Encryption Key Transmission	3G-Web receives a request from EC site, creates an encryption key for consumer (Hereinafter, browser encryption key) and for EC site respectively and returns it to EC site.
3	Redirect	EC site sends order ID, browser encryption key and URL of 3G-Web to consumer, and prompts the consumer to redirect to 3G-Web payment page. ∗ When displaying the 3G-Web payment page, instead of displaying the pop-up on a different page, display it on the same page.
4	Payment Information Input	Consumer selects the Payment type and inputs the request information. After selecting payment type, consumer browser redirects to the payment confirmation page.
5	Payment Request	Consumer makes payment request.
6	Result Notification	3G-Web sends the result notification to EC site in POST format.
7	Payment Completion	When consumer clicks the button “Return to EC site”, 3G-Web redirects to EC site’s payment completion Page.
8	Payment Notification	Notifies payment notification to EC site once VeriTrans3G verifies the payment has been received from the consumer, for that particular transaction. The notification is sent in POST format.

Table 2-4-7 3G-Web Integration Process Overview (Bank Payment (ATM))

[Bank Payment (Internet Banking PC)]

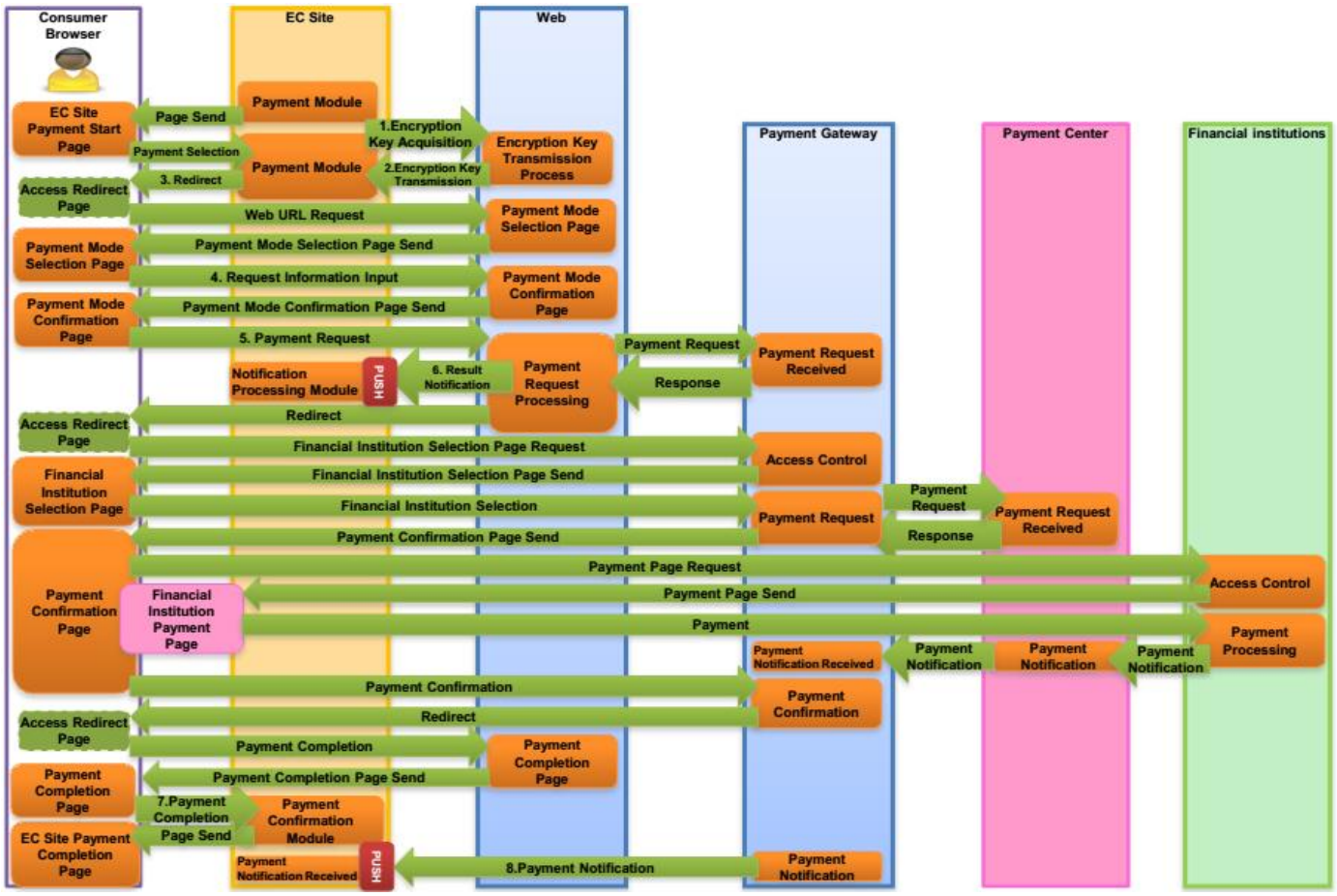

Figure 2-4-8 System Process Overview Diagram when Using 3G-Web (Bank Payment (Internet Banking PC))

No.	Basic Functions	Description
1	Encryption Key Acquisition	Sends payment request received from request module of EC site to 3G-Web.
2	Encryption Key Transmission	3G-Web receives a request from EC site, creates an encryption key for consumer (Hereinafter, browser encryption key) and for EC site respectively and returns it to EC site.
3	Redirect	EC site sends order ID, browser encryption key and URL of 3G-Web to consumer, and prompts the consumer to redirect to 3G-Web Payment Page. ∗ When displaying the 3G-Web payment page, instead of displaying the pop-up on a different page, display it on the same page.
4	Payment Information Input	Consumer selects the Payment type and inputs the request information. After selecting payment type, consumer browser redirects to the payment confirmation page.
5	Payment Request	Consumer makes payment request.
6	Result Notification	3G-Web sends the result notification to EC site in POST format.
7	Payment Completion	When consumer clicks the button “Return to EC site”, 3G-Web redirects to EC site’s payment completion page.
8	Payment Notification	Notifies payment notification to EC site once VeriTrans3G verifies the payment has been received from the consumer, for that particular transaction. The notification is sent in POST format.

Table 2-4-8 3G-Web Integration Process Overview (Bank payment (Internet Banking PC))

[Bank Payment (Internet Banking Mobile)]

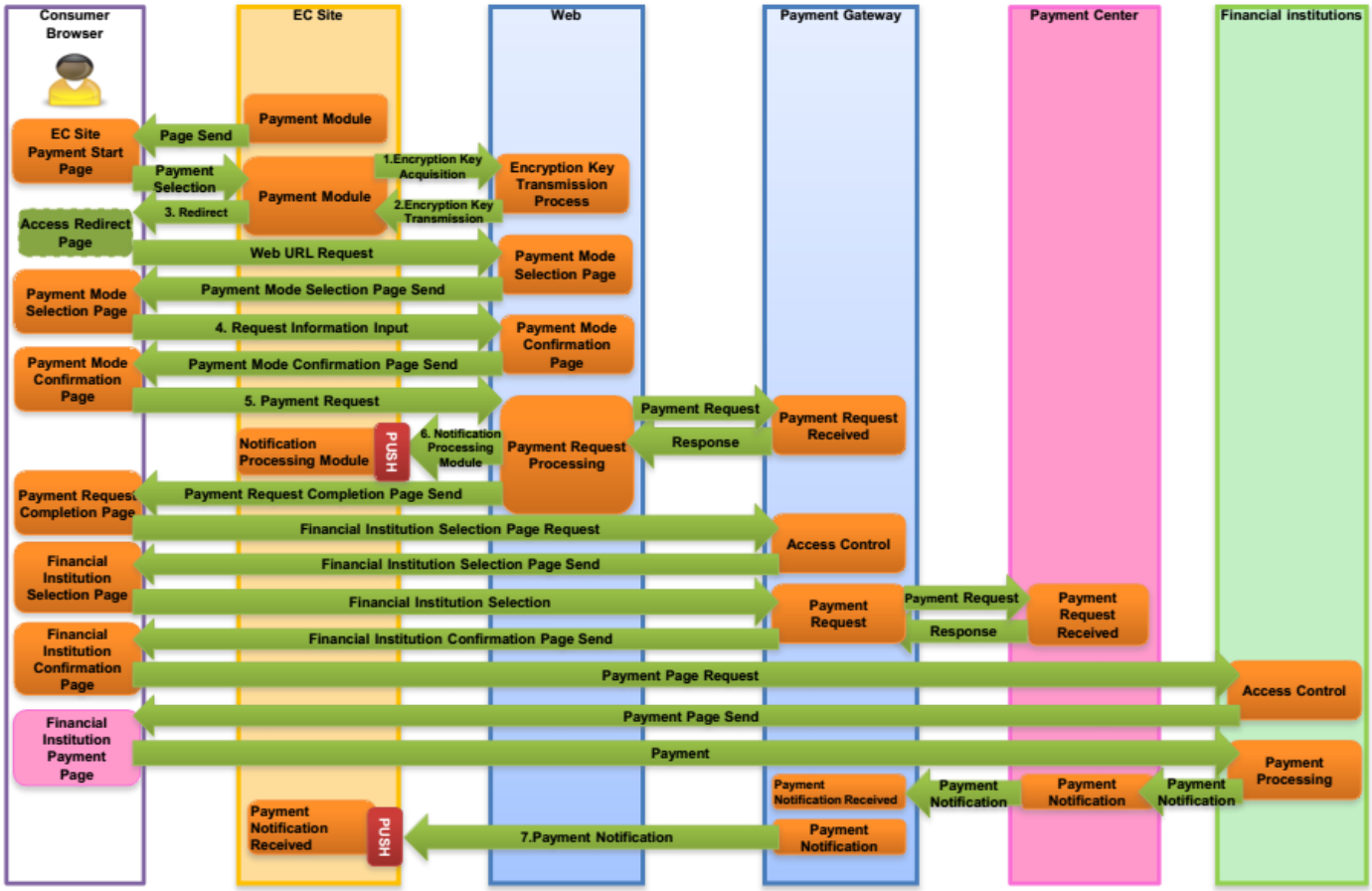

Figure 2-4-9 System Process Overview Diagram when Using 3G-Web (Bank payment (Internet Banking Mobile))

No.	Basic Functions	Description
1	Encryption Key Acquisition	Sends payment request received from request module of EC site to 3G-Web.
2	Encryption Key Transmission	3G-Web receives a request from EC site, creates an encryption key for consumer (hereinafter, browser encryption key) and for EC site respectively and returns it to EC site.
3	Redirect	EC site sends order ID, browser encryption key and URL of 3G-Web to consumer, and prompts the consumer to redirect to 3G-Web Payment Page. ∗ When displaying the 3G-Web payment page, instead of displaying the pop-up on a different page, display it on the same page.
4	Payment Information Input	Consumer selects the Payment type and inputs the request information. After selecting payment type, consumer browser redirects to the payment confirmation page.
5	Payment Request	Consumer makes payment request. When consumer makes payment request, consumer browser redirect to financial institution selection page of VeriTrans3G.
6	Result Notification	3G-Web sends the result notification to EC site in POST format.
7	Payment Notification	Notifies payment notification to EC site once VeriTrans3G verifies the payment has been received from the consumer, for that particular transaction. The notification is sent in POST request.

Table 2-4-9 3G-Web Integration Process Overview (Bank payment (Internet Banking Mobile))

Chapter 3 Handling Result Notification

3-1 Target of Result Notification Process

3.1.1 Result Notification Process from 3G-Web

3G-Web identifies the status of payment result (or payment request) and sends a PUSH result notification to the merchant (EC site).

In this result notification, irrespective of the payment result, notification is sent for all the transactions.

The result notification is sent using the HTTP POST method.

The result notification from 3G-Web is sent to 'Payment Result Notification URL' specified in the request message to 3G-Web from merchant. If the URL is not specified in the request message, it is sent to the 'Payment Result Notification URL' which was registered at the time of application.

The process(source code), which is required for handling the result notification from 3G-Web, is given in the sample program. Merchants can use the sample programs by customizing it as per their own requirements. (Please note that customization is to be done at merchant's end).

∗ **Supported protocol is HTTP (Port: 80), HTTPS (Port: 443).**
Other protocols and port combinations are not supported.

If you would like to receive the result notification by HTTPS, please make sure that SSL configuration setup is done at merchant-side server. Please use the SSL certificate that has been issued by the certificate authority.

∗ **Please note that Self-Sign SSL Certificate cannot be used.**
At the time of connection from 3G-Web, if error occurs during certification check and result notification is suspended.

After receiving result notification, please return HTTPS status code "200" according to the format of the response message of HTTP protocol.

∗ **If the status is other than HTTP status code "200" or there is no response from the server, it is treated as a notification error and notification continues the retries up to the upper limit registered at the time of merchant registration (upper limit of payment result notification retry count).**

3.1.2 Result Notification Process from VeriTrans3G

In certain payment services PUSH notifications will be sent directly from VeriTrans3G to the merchant (EC site) due to consumer action result or a change in a status of transaction in VeriTrans3G, other than the result notification from 3G-Web.

VeriTrans3G will send PUSH notifications to the merchant after receiving result notification from each payment center.

Payment Service	Result Notification	Description
Credit card	-	-

Convenience store	Payment notification	Notifies payment completion to merchant (EC site) once VeriTrans3G receives payment completion notification from convenience store payment center. Consider this payment notification as confirmation of funds received and carry out the shipping process etc at the timing of receiving this notification.
E-Money	Payment notification	Notifies payment completion to merchant (EC site) once VeriTrans3G receives payment completion notification from E-Money payment center. Consider this payment notification as confirmation of funds received and carry out the shipping process etc at the timing of receiving this notification.
Bank	Payment notification	Notifies payment completion to merchant (EC site) once VeriTrans3G receives payment completion notification from bank payment center. Consider this payment notification as confirmation of funds received and carry out the shipping process etc at the timing of receiving this notification.

Table 3-1-2 Result Notification by Service Matrix (PUSH Notifications from VeriTrans3G))

For details of the result notification process from VeriTrans3G, please refer to the [VeriTrans3G Development Guide].

It should be noted that, merchants should implement the notification handling process at their end (EC site). For this, sample source codes are given in MDK sample programs of VeriTrans3G. Please download it from the support site of VeriTrans3G.

Chapter 4 Interface Details

This chapter explains about the messages used in 3G-Web.

Each item is URL encoded in the character code UTF-8 format.

4-1 Access URL

Access URL (Secure Environment)	
For encryption key acquisition	https://pay.veritrans.co.jp/web1/commodityRegist.action
For 3G-Web redirect	https://pay.veritrans.co.jp/web1/deviceCheck.action
∗ To access this URL, the client that supports TLS1.1 or TLS1.2 is mandatory.	

Please use the following provisional environment URL if you want to support devices like feature phones etc which does not support TLS1.1 or TLS1.2.

However, we are planning to stop access to this URL in May 2018, till that you will need to switch to a secure environment mentioned above.

Access URL (Provisional Environment SSL3.0/TLS1.0 Enabled)	
For encryption key acquisition	https://3gs.veritrans.co.jp/web1/commodityRegist.action
For 3G-Web redirect	https://3gs.veritrans.co.jp/web1/deviceCheck.action
∗ SSL3.0/TLS1.0 is enabled for these URL's. ∗ We are planning to stop access to this environment in May 2018.	

Note) The merchant who is already using 3G-Web service but is still using old environment (URL is https://3g.veritrans.co.jp), will need to switch to the above-mentioned new URL by August 2016.

For further details, please contact us by E-mail on below given addresses.

[Contact Details]

VeriTrans Inc. SSL-SHA2 Migration Helpdesk E-mail: ssl-sha2@veritrans.jp

Or

VeriTrans Inc. Technical Support E-mail: tech-support@veritrans.jp

4-2 Encryption Key Acquisition

Below are the contents of the request/response in step (5) (6) of 'Figure 2-3-1 Sample Program '.

∗ Personal information is the information of the payer. Please note consumer and the payer can be different.

As 3G-Web supports various payment types, the mandatory fields / optional fields may change according to payment type / payment sub-type (See below).

- The contents of "Settings" column are as follows.

  Request message … Mandatory field: ○ Optional field: Δ

  See below: ∗ (It changes according to payment type / payment sub-type. Please refer to the [Request Message Setting Item List].)

(5) Request Message: EC Site → 3G-Web				
URL: https://*.veritrans.co.jp/web1/commodityRegist.action				
Field Name	**Item Name**	**Format / Limitations**	**Description**	**Settings**
MERCHANT_ID	Merchant ID	Single byte alphanumeric characters; 22 characters or less	Specifies merchant ID issued by VeriTrans.	○
ORDER_ID	Order ID	Single byte alphanumeric characters symbols; 100 characters or less	Merchants assigns a (unique) number to the order ID. It is mandatory for processing each request. Please assign the number such that no two order IDs have the same number. It cannot be duplicated even if the payment services are different. * Beside single byte alphanumeric characters, only “-” (hyphen) and “_” (underscore) symbols can be used.	○
MERCHANTHASH	Merchant generated hash value	-	A generated sha512 hash value by combining merchant hash seed, Merchant ID, Payment Type, Order ID and Amount with comma separator.	○
SESSION_ID	Session ID	Single byte alphanumeric characters; 50 characters or less	A random number that is arbitrarily set by merchant.	○
AMOUNT	Purchase amount	Single byte numbers; 9 digits or less	***1**	○
FINISH_PAYMENT_ACCESS_URL	Payment result notification URL	Single byte alphanumeric characters symbols; 256 characters or less	This is a notification URL that can be set per request message from EC Shop which is used in step (11) of “Figure 2-3-1 Sample Program ”. Query string cannot be specified.	Δ
FINISH_PAYMENT_RETURN_URL	Return URL after payment completion	Single byte alphanumeric characters symbols; 256 characters or less	This is a return URL to the EC site when the payment is successfull. Query string and anchor cannot be specified.	Δ
UNFINISH_PAYMENT_RETURN_URL	Return URL after payment is not done	Single byte alphanumeric characters symbols; 256 characters or less	This is a return URL to return to EC site when consumer does not carry out payment. Query string and anchor cannot be specified.	Δ
ERROR_PAYMENT_RETURN_URL	Return URL at the time of error in payment	Single byte alphanumeric characters symbols; 256 characters or less	This is a URL to return to EC site when there is error in payment. Query string and anchor cannot be specified.	Δ
DUMMY_PAYMENT_FLAG	Dummy order flag	Single byte numbers; 1 digit	Dummy order flag. If not specified, it is assumed to be “0”. “0”: Live order “1”: Dummy order	Δ

SETTLEMENT_TYPE	Payment type	Single byte numbers; 2 digits	“00”: Payment type not specified “01”: Card Payment “02”: Convenience Store Payment “03”: E-Money Payment “04”: Bank Payment	○
SETTLEMENT_SUB_TYPE	Payment sub-type	Single byte numbers; 3 digits	When convenience store payment is selected from Payment type options “201”: 7-Eleven “205”: econtext (LAWSON, FamilyMart, MINISTOP, Seicomart, Circle K Sunkus) “204”: Other (Daily YAMAZAKI) When E-Money payment is selected from Payment type options “311”: PC Edy “312”: Mobile Edy “321”: PC Suica “322”: Mobile Suica “331”: PC WAON “332”: Mobile WAON When bank payment is selected from Payment type options “411”: ATM payment “420”: Internet banking payment	*
LANG_ENABLE_FLAG	Language selection enable flag	Single byte numbers; 1 digit	“0”: Un-selectable “1”: Selectable	Δ
LANG	Payment page language	See Remarks	Specify the following available languages with comma-separation “ja”: Japanese “en”: English “zh”: Chinese	Δ
CARD_INSTALLMENT_JPO	Card payment option	Single byte numbers; 2 digits or less	Card ayment options that merchant can use For example: “10”: Lump-sum payment “21”: Lump-sum bonus “61”: Installment “80”: Revolving payment	*

CARD_INSTALLMENT_JPO_CNT	Number of Card installments	Single byte numbers; 2 digits or less	Number of installments that merchant can use For example: “03”: 3 times “06”: 6 times “10”: 10 times “12”: 12 times “15”: 15 times “16”: 16 times “18”: 18 times “20”: 20 times “24”: 24 times * This can be specified only when CARD_INSTALLMENT_JPO is 61.	*
CARD_CAPTURE_FLAG	Card capture flag	Single byte numbers; 1 digit	“0”: Authorize only “1”: Authorize and Capture	*
DDD_ENABLE_FLAG	3-D Secure enable flag	Single byte numbers; 1 digit	3-D Secure enablement flag. In credit card payment, this flag is used to indicate whether to opt in for 3-D Secure transaction. If not set, it is assumed to be “1”. This can be set per request. “0”: Not to use 3-D Secure “1”: Use 3-D Secure (Only if registered)	*
SHOP_NAME	Shop name for Mobile Edy	String; 48 bytes or less	This is a shop name used in payment request E-mail and payment completion E-mail.	*
SCREEN_TITLE	Item name for Suica	String; 40 bytes or less	String displayed in “Item / service name” on payment completion page / payment confirmation page.	*
CONTENTS	Billing contents	Double byte; 12 characters or less	These contents will be displayed on ATM terminal.	*
CONTENTS_KANA	Billing contents in Kana	Double byte Kana; 24 characters or less	These kana contents will be displayed on ATM terminal..	*
TIMELIMIT_OF_PAYMENT	Payment deadline	Single byte numbers; 8 digits	YYYYMMDD Format ***2**	*
TIMELIMIT_OF_CANCEL	Payment cancellation expiration	Single byte numbers; 8 digits	YYYYMMDD Format ***3**	*
Below, only the Item number set repeatedly				
COMMODITY_ID	Item ID	Single byte alphanumeric characters; symbols; 15 characters or less	Mandatory when unit price, item quantity, item name input field exist	Δ
COMMODITY_UNIT	Unit price	Single byte numbers; 9 digits or less	If not set, it will not appear on 3G-Web payment confirmation page, so setting is recommended.	Δ
COMMODITY_NUM	Item quantity	Single byte numbers; 4 digits or less		Δ
COMMODITY_NAME	Item name	String; 50 bytes or less		Δ
JAN_CODE	JAN code	Single byte alphanumeric characters; symbols; 30 characters or less	In case of unit price, item quantity, item name input field exist, JAN code can be specified whenever necessary.	Δ

***1:** The following are the details of the upper limit and lower limit of payment amounts. Following that are the limitations, in case payment type is specified.

However, if the payment type is not specified or if the serviceOptionType (Payment service option) is not specified in E-Money payment, the upper limit of the smallest amount among the available payment types will be used.

■ Credit Card Payment

1 to 99,999,999

■ Convenience Store Payment

1 to 299,999

■ E-Money Payment

Edy: 1 to 50,000

Suica: 1 to 20,000

WAON: 1 to 50,000

■ Bank payment

1 to 999,999,999

***2:** Following are the details of payment deadline. Following are the limitations in case the payment type is specified.

However, if the payment type is not specified or if the payment sub-type is not specified in convenience store payment, it will be the shortest time limit (From transaction day ~ 60 days) will be considered.

■ Convenience Store Payment

7-Eleven:	From transaction day ~ 150 days
LAWSON, FamilyMart, Seicomart:	From transaction day ~ 60 days
Other:	From transaction day ~ 365 days

■ E-Money Payment

From transaction day ~ 90 days

■ Bank Payment

From transaction day ~ 60 days

***3:** In case of WAON, the deadline is not for the cancellation but it is for the refund. It is till 365th day's 23:59:59 from the day of payment. E.g. if the transaction is done on 1/1 (1st January), the deadline will be YYYY1231 (31st December of the same year).

[Request Message Setting Item List]

Mandatory field: ○

Optional fields (Mandatory at the time of payment): □ (Although it is an optional field in request message, if it is not set, it

becomes mandatory for consumer on payment page)

Optional fields (Supplementary at the time of payment): ◊ (Although it is an optional field in request message, if it is not set, 3G-Web will use default values)

Optional fields (Optional at the time of payment): Δ (Optional fields at the time of request message, as well as on payment page)

Settings disabled: X (Even if is set, payment request will not be declied, but this item is not used in payment.)

(5) Request Message: EC SITE → 3G-Web

Field Name	Payment types / Payment Sub-Type												
				E-Money							Bank		
	Not Specified	Card	Convenience Store	Not Specified	PC Edy	Mobile Edy	PC Suica	Mobile Suica	PC WAON	Mobile WAON	Not Specified	ATM	Internet Banking
SETTLEMENT_SUB_TYPE	X	X	Δ	X	○	○	○	○	○	○	X	○	○
CARD_INSTALLMENT_JPO	X	□	X	X	X	X	X	X	X	X	X	X	X
CARD_INSTALLMENT_JPO_CNT	X	□	X	X	X	X	X	X	X	X	X	X	X
CARD_CAPTURE_FLAG	◊	◊	X	X	X	X	X	X	X	X	X	X	X
DDD_ENABLE_FLAG	◊	◊	X	X	X	X	X	X	X	X	X	X	X
SHOP_NAME	Δ	X	X	Δ	X	Δ	X	X	X	X	X	X	X
SCREEN_TITLE	∗1	X	X	∗1	X	X	○	○	X	X	X	X	X
CONTENTS	∗2	X	X	X	X	X	X	X	X	X	○	○	○
CONTENTS_KANA	∗2	X	X	X	X	X	X	X	X	X	○	○	○
TIMELIMIT_OF_PAYMENT	Δ	X	◊	◊	X	◊	◊	◊	◊	◊	◊	◊	◊
TIMELIMIT_OF_CANCEL	∗3	X	X	∗3	X	X	X	X	○	○	X	X	X

∗**1**: It is mandatory item in case of Suica Payment (PC Suica / Mobile Suica).

∗**2**: It is mandatory item in case of Bank Payment (ATM / Internet Banking).

∗**3**: It is mandatory item in case of WAON Payment (PC WAON / Mobile WAON).

■ The contents of “Settings” column are as follows.

Response message …Conditional return: ∗

(6) Response Message: 3G-Web → EC SITE

Field Name	Item Name	Format / Limitations	Details	Settings
MERCHANT_ENCRYPTION_KEY	Merchant encryption key	Single byte alphanumeric characters; 120 or less	Encryption Key that EC site stores (saves) ∗ Returns when successful	∗
BROWSER_ENCRYPTION_KEY	Browser encryption key	Single byte alphanumeric characters; 120 characters or less	Encryption Key returned to browser ∗ Returns when successful	∗
ERROR_MESSAGE	Error message	Please refer to the description in the separate document	Error message that 3G-Web returns ∗ Returns when error occurs	∗

∗ “Merchant Encryption Key” is not used in payment process. But please keep it safe, as it may be required in case of payment information inquiry.

4-3 3G-Web Redirect

Fields used for redirection to consumer browser in step (9) of “Figure 2-3-1 Sample Program ” are as follows.

- The contents of “Settings” column are as follows.

  Redirect Message … Always redirect: ○

(9) Redirect Message: EC site → Consumer Browser				
URL: https://*.veritrans.co.jp/web1/deviceCheck.action				
Field Name	**Item Name**	**Format / Limitations**	**Description**	**Settings**
MERCHANT_ID	Merchant ID	Single byte alphanumeric characters; 22 characters or less	ID that identifies the merchant	○
ORDER_ID	Order ID	Single byte alphanumeric characters; symbols; 100 characters or less	ID to identify the order of merchant	○
BROWSER_ENCRYPTION_KEY	Browser encryption key	Single byte alphanumeric characters; 120 characters or less	Encryption key returned to the browser	○

4-4 Payment Result Verification

It is sent from the consumer browser to EC site in step (14) of “Figure 2-3-1 Sample Program ”. EC-Shop should consider a payment as a successful payment if it redirect from consumer browser implies ‘payment result is successful’ and also status matches with the payment notification received in “4-5 Result Notification Message from 3G-Web”.

A return URL to EC site from consumer browser can be set in request message of “4-2 Encryption Key Acquisition”. If URL is not set in request message, then URL, which was specified at the time of merchant registration, will be used. It will return to the following URL depending on the payment completion or error occurrence.

When payment is completed: Return URL after payment completion

When consumer did not make a payment: Return URL at the time of payment is not made

When payment ended with an error: Return URL at the time of error in payment

Contents sent from consumer browser are as follows.

■ The contents of “Settings” column are as follows.

Information Receiving…Always received: ○ Other conditions applied: ＊ (Conditions are explained in Detail column)

(14) Transmission Information: Consumer Browser → EC Site				
Field Name	**Item Name**	**Format / Limitations**	**Description**	**Settings**
orderId	Order ID	Single byte alphanumeric characters; symbols; 100 characters or less	Order ID that was sent from EC site	○
mStatus	Status	Please refer to the 4.5.2	Please refer to the 4.5.2 ＊ It is returned only in case of success and in case of error. It will not be returned in case of payment not made.	＊
vResultCode	Result code	Please refer to the 4.5.2	Please refer to the 4.5.2 ＊ It is returned only in case of success and in case of error. It will not be returned in case of payment not made.	＊
sessionId	Session ID	Please refer to the 4-2	SESSION ID transmitted in 4-2 ＊ It is returned only in case of success and in case of error. It will not be returned in case of payment not made.	＊

4-5 Result Notification Message from 3G-Web

4.5.1 Overview of Result Notification Message

■ **Functional Overview**

3G-Web sends the PUSH result notification to EC site, when the status of payment result (or payment request result) becomes clear.

The result notification is sent in HTTP POST.

＊ **Protocol supports HTTP (Port: 80) and HTTPS (Port: 443).**

Please refer to the “Chapter 3 Handling Result Notification ” in this guide for Process Overview.

■ **About result notification process result**

If the EC site returns the HTTP status code “200” for the notification sent from 3G-Web, it is considered as EC site has received the notification successfully.

If the status code other than “200” is returned, it is considered as failure in sending notification and 3G-Web retries up to the upper limit registered at the time of merchant registration (upper limit of payment result notification retry count).

＊ **Notifications will be stopped when upper limit of retry count is reached.**

＊ **HMAC value (content-hmac) is not included in result notification message from 3G-Web.**

4.5.2 Result Notification

Notification parameter to EC site from 3G-Web in step (11) of “Figure 2-3-1 Sample Program ” are as follows.

∗ **Result notification fields from 3G-Web are limited to following items only. Merchant cannot add any other field on his own.**

■ Contents of “Settings” column are as follows.

Information Receiving… Always receive: ○ Receiving depending on situation: Δ

11) Information Receiving: 3G-Web → EC Site				
Field Name	**Item Name**	**Format / Limitations**	**Description**	**Settings**
orderId	Order ID	Single byte alphanumeric characters; symbols, 100 characters or less	Order ID sent from EC site	○
mStatus	Status	Please refer to the description in the right column	Order processing status “success”: Successful completion “failure”: Failure in completion “pending”: On hold	○
mErrMsg	Message	Please refer to the description in the separate document	Order processing message * In credit card payment (With 3-D Secure)), this value is not sent. * Payment other than Credit Card Payment (With 3-D Secure)), it is always sent.	Δ
vResultCode	Result code	Please refer to the description in the separate document	Code that represents the process result in detail	○
userName	User name in Kanji	Double byte; 20 characters or less	The value entered on 3G-Web payment page is returned. * For more details refer to the following “Returning of input value”.	Δ
userNameKana	User name in Kana	Double byte Kana; 20 characters or less		Δ
mailAddress	Email address	Single byte alphanumeric characters; symbols; 50 characters or less		Δ
telephoneno	Telephone number	Single byte numbers; 11 digits or less		Δ

➢ Returning of Input Value

The payment type and information returned is as follows.

- User Name in Kanji: Convenience Store Payment, Bank Payment
- User Name in Kana: Convenience Store Payment, Bank Payment
- Email Address: E-Money Payment
- Telephone Number: Convenience Store Payment

Moreover, please note that these values are not returned in credit card Payment (with or without 3-D Secure).

4-6 Result Notification Message from VeriTrans3G

Please refer to the “Table 3-1-2 Result Notification by Service Matrix (PUSH Notifications from VeriTrans3G) ” which lists the services for which notification is sent from VeriTrans3G.

Please refer to the [VeriTrans3G Development Guide] for Overview of Result Notification Message and Interface Details of Result Notification Message for each type of Payment Service.

Chapter 5 Other - Supplementary Items

5-1 Notes for Testing

For test specification details, please refer to the “VeriTrans3G Integration Test Guide”.

Following are the notes for test implementation.

- When executing test transactions, always set the “Dummy transaction flag” to “1”.
  In “(5) Request Message: EC SITE → 3G-Web” of “4-2 Encryption Key Acquisition”, set the “DUMMY_PAYMENT_FLAG (Dummy Transaction Flag)” to ““1”: Dummy Transaction”.

- For executing test transactions it is required to use specified credentials (given card number, given payment amount, etc.). For testing credentials, please refer to the "VeriTrans3G Integration Test Guide".

- At the time of transaction testing, please note the following.
  - Order ID (orderId): Specify any random value. Order ID should be unique. In addition, the Order ID used in test transaction cannot be re-used in live orders.
  - Amount: Please set a valid amount data. (Numerical values with decimal points are not allowed)
  - Live request for dummy order and dummy request for live order results in error.

- Selection Options for “Year (Last 2 digits) of “Card expiry” on (“Select Payment type (Credit Card Payment)” Page
  For the selection options of “Card Expiry” on “Select Payment type (Credit Card Payment)” Page, in case of dummy mode, "90" - "99" is displayed in the value of "Year (Last two digits)" for testing of abnormal test cases.

Figure 5-1-1 Selection Options of “Card Expiry” on “Select Payment Mode” Page

∗ In the dummy mode, for testing of abnormal test cases, specific error code is returned with specific value of "Card Expiry". Please refer to the “VeriTrans3G Integration Test Guide” for details.

∗ In live order, values of “Year (Last two digits), “From the current year – Year 1” to “Next 15 years, including current year” are displayed.

Example) Current Year: Year 2016

→ In Selection Options Year (20)15 to Year (20)30 are displayed.

5-2 Verification of Test Transaction Results on MAP

Merchant can use Merchant administration portal (MAP) to search a specific transaction or check the transaction status. For more details, please refer to the “Usage Guide”.

∗ About MAP

MAP stands for Merchant Administration Portal; it is a Web-based management tool that provides a variety of information and functions for managing and operating on VeriTrans3G.

URL: https://pay.veritrans.co.jp/maps/