

Part 2: Service Information
Card Payment
1. Domain Name / URL to apply for service
<p>Application via Website/Mobile Application (e.g., http://www.kasikornbank.com):</p> <p>_____</p> <p>Remarks: The name of the website or mobile application registrant must be the name of the shop owner (in case of natural person) / juristic person or managing director/managing partner who is authorized signatory per the Certificate of Registration (in case of juristic person).</p>
2. Details of Card Acceptance (You may select more than one item)
<p><input type="checkbox"/> 2.1 Acceptance of Full Payment (Please select only one*)</p> <p style="margin-left: 20px;"><input type="checkbox"/> The merchant is responsible for the collection fees (MDR).</p> <p style="margin-left: 20px;"><input type="checkbox"/> The payer is responsible for the collection fees (MDR) - Convenience Fee; the collection fees (MDR) shall include VAT.</p> <p style="margin-left: 20px;">Remarks: If not specified by the merchant, the merchant agrees to be responsible for the MDR fee.</p> <p>2.1.1 Types of Cards</p> <p style="margin-left: 20px;"><input type="checkbox"/> Visa * 3D Secure service</p> <p style="margin-left: 20px;"><input type="checkbox"/> MasterCard * 3D Secure service</p> <p style="margin-left: 20px;"><input type="checkbox"/> JCB * 3D Secure service</p> <p style="margin-left: 20px;"><input type="checkbox"/> TPN / UnionPay</p> <p style="margin-left: 20px;"><input type="checkbox"/> AMEX</p> <p style="margin-left: 20px;">Remarks:</p> <p style="margin-left: 40px;">1. 3D Secure is the security standard for the payer with authentication processes upon goods/service payment to prevent unauthorized card usage.</p> <p style="margin-left: 40px;">2. If the merchant wants to use non-3D Secure service for card acceptance, KBank shall consider the request on a case-by-case basis, and the merchant shall prepare a letter stating its agreement to assume the burden of related risks per KBank's established pattern and method.</p> <p style="margin-left: 40px;">3. If not specified by the merchant, the merchant agrees to accept goods/service payment with Visa / MasterCard / JCB card only.</p> <p>2.1.2 Credit card issuing countries (Please select only one as related to the currency chosen on Page 2)</p> <p style="margin-left: 20px;"><input type="checkbox"/> Thailand only (Selecting for MCC with THB currency only)</p> <p style="margin-left: 20px;"><input type="checkbox"/> Foreign countries only (Selecting for DCC and/or MCC)</p> <p style="margin-left: 20px;"><input type="checkbox"/> All countries (Selecting for DCC and/or MCC)</p> <p style="margin-left: 20px;">Remarks: If not specified by the merchant, the merchant agrees to accept cards of all countries worldwide</p>

Appendix: Card Payment

4. Merchant Portal Information	
Level of User	Permitted Usage
Admin User	Transactions and data inquiries, settlements, voiding of transactions and correction of data, and receiving of codes for system connection
Normal User	Transactions and data inquiries only

Please specify the permitted usage and Username as desired
(Username must be an email address for each level of user that has not been used with K-Payment Gateway system)

	Username (in block letters)	Level of User
1	_____	
2	_____	
3	_____	
4	_____	
5	_____	
6	_____	

5. Merchant Website Information (KBank advises that this part should be filled in by the merchant's technical administrator.)

Does the merchant want real-time response after approvals from KBank? (Please select only one)

Yes - KBank will send the response after approvals to the merchant's server in real-time (SSL/TLS must be installed).

No - Online Merchant Report – The merchant can check the information of purchases via the Online Merchant Report system.

If you want real-time confirmation, please provide the following information:

1. Response URL of the merchant for receiving response messages from KBank
(e.g., <https://www.KBank.com/rec.asp>):

Callback URL _____

Notify URL _____

2. IP Address of the merchant for receiving response messages from KBank (e.g., 203.151.145.1):

3. Security protocol for data transmission on internet networks

TLS 1.2 or higher Others (please specify)

4. Certification Authority (CA):

Verisign Entrust Baltimore CyberTrust

Thawte Others (please specify)

Appendix: Card Payment

Issue date (dd/mm/yy)/...../..... Expiry date (dd/mm/yy)/...../.....

The merchant: has TLS on their own server.

shares the TLS system of a host server (e.g., that of Web Hosting service provider).

Does the merchant want to use tokenization service to enhance security of card data? Yes No

Remarks: If the merchant wants to keep the cardholder's card data, PCI DSS document must be attached for consideration.

6. System Developer for Merchant

Name of system developing company _____

Name of system developer _____

Email address (in block letters) _____

Contact telephone number _____

7. Other Service Conditions (for Bank use)
