

Title

Concept Paper – Debit Card-i Requirements

Effective Date

The consultation period of this concept paper ends on 8 March 2013

Applicability

All issuers and acquirers of debit card-i

Summary

This concept paper outlines specific requirements, minimum standards and risk management principles to be observed by debit card issuers and acquirers. Bank Negara Malaysia (the Bank) invites constructive feedback on this concept paper. To facilitate the Bank's assessment, each comment should be supported with a clear rationale, accompanying evidence or illustration, and proposed alternative. The industry is required to respond to the Bank latest by 8 March 2013.

Issuing Department

Jabatan Dasar Sistem Pembayaran
Jabatan Konsumer dan Amalan Pemasaran
Islamic Banking and Takaful Department

[Guideline Info](#)

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements
-----------------	---	---

OVERVIEW	2
1. INTRODUCTION	2
2. LEGAL PROVISIONS	2
3. SCOPE	2
4. APPLICABILITY	2
5. DEFINITION	2
PART 1	4
A. FEES AND CHARGES	4
6. GUIDING PRINCIPLE ON FEES AND CHARGES.....	4
B. DISCLOSURE AND TRANSPARENCY REQUIREMENTS	4
7. PRE-CONTRACTUAL STAGE	4
8. AT THE POINT OF ENTERING INTO A CONTRACT	5
9. DURING THE TERM OF THE CONTRACT	7
C. LIABILITY	8
10. LIABILITY FOR UNAUTHORISED TRANSACTIONS.....	8
D. MARKETING REQUIREMENTS	9
11. ADVERTISEMENT	9
12. ISSUER's OTHER OBLIGATIONS.....	10
E. OTHER REQUIREMENTS	10
13. CUSTOMER INFORMATION.....	10
14. COMPLAINTS MANAGEMENT.....	11
15. USAGE OF DEBIT CARD-i FOR UNLAWFUL ACTIVITIES	11
PART 2	11
F. RISK MANAGEMENT	11
16. EFFECTIVE MANAGEMENT OVERSIGHT.....	11
17. COMPREHENSIVE SECURITY POLICIES, PROCEDURES AND CONTROLS	12
18. ROBUST OPERATIONAL RELIABILITY AND BUSINESS CONTINUITY	15
19. OUTSOURCING RISK MANAGEMENT	16
20. FRAUD RISK MANAGEMENT	17
21. SPECIFIC REQUIREMENTS FOR ACQUIRERS	21
22. COMPLIANCE WITH OTHER REQUIREMENTS	23
G. APPROVED SHARIAH CONCEPT APPLIED IN DEBIT CARD-i	23
23. SHARIAH CONCEPT.....	23
APPENDICES	25

BNM/RH/CP 008-9	<ul style="list-style-type: none">• Payment Systems Policy Department• Consumer & Market Conduct Department• Islamic Banking and Takaful Department	Concept Paper - Debit Card-i Requirements	Page 1/26
-----------------	---	---	-----------

This concept paper outlines specific requirements, minimum standards and risk management principles to be observed by debit card-i issuers and acquirers.

Bank Negara Malaysia (the Bank) invites constructive feedback on this concept paper. To facilitate the Bank's assessment, please support each comment with a clear rationale, accompanying evidence or illustration, and proposed alternative. Please respond to the Bank latest by 8 March 2013 addressed to:

Pengarah
Jabatan Dasar Sistem Pembayaran
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 2/26
-----------------	---	---	-----------

OVERVIEW

1. INTRODUCTION

1.1 These requirements aim to safeguard the integrity of the debit card-i system, thereby preserving consumer confidence and promoting its wider adoption in Malaysia.

2. LEGAL PROVISIONS

2.1 These requirements are issued pursuant to:

- a. Sections 5, 25 and 70 of the Payment Systems Act 2003 (PSA);
- b. Section 126 of the Banking and Financial Institutions Act 1989 (BAFIA);
- c. Section 53A of the Islamic Banking Act 1983 (IBA); and
- d. Section 126 of the Development Financial Institutions Act 2002 (DFIA).

3. SCOPE

3.1 Part 1 outlines specific requirements and minimum standards to be observed by debit card-i issuers and acquirers while Part 2 outlines the risk management principles and requirements for debit card-i issuers and acquirers.

4. APPLICABILITY

4.1 These requirements are applicable to all debit card-i issuers and acquirers.

5. DEFINITION

5.1 For the purpose of these requirements, the following terms are defined as follows:

5.1.1 *Debit card-i* refers to a payment instrument based on Shariah principles that is linked to a deposit account at a financial institution, and used to pay for goods and services and/or withdraw cash from automated teller machines or withdraw cash at participating retail outlets through debit card-i usage (cash out) by debiting the cardholder's account.

5.1.2 *Issuer* refers to a financial institution which issues debit card-i.

BNM/RH/CP 008-9	<ul style="list-style-type: none">• Payment Systems Policy Department• Consumer & Market Conduct Department• Islamic Banking and Takaful Department	Concept Paper - Debit Card-i Requirements	Page 3/26
-----------------	---	---	-----------

5.1.3 *Acquirer* refers to any person that enters into a contractual relationship with the merchant for the purpose of accepting debit card-i for payment.

5.1.4 *Financial institution* refers to any person licensed under the BAFIA and IBA or prescribed under the DFIA.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 4/26
-----------------	---	---	-----------

PART 1

A. FEES AND CHARGES

6. GUIDING PRINCIPLE ON FEES AND CHARGES

6.1 In determining the type and quantum of fees and charges on debit card-i, issuers are required to ensure compliance with the Guidelines on Imposition of Fees and Charges on Financial Products and Services.

6.2 Upon the issuance of a debit card, issuers may impose a fee for the card. However, issuers must not charge cardholders an annual fee during the same year the debit card is issued.

B. DISCLOSURE AND TRANSPARENCY REQUIREMENTS

This section should be read together with the general policy requirements stipulated in the Guidelines on Product Transparency and Disclosure.

Disclosure is effective when product information is given to the cardholders at a time that is most relevant to enable the cardholders to make informed decisions at each of the three stages of the contractual process.

Issuers are required to provide a product disclosure sheet (as per the format provided in Appendix 1) containing key information for cardholders to make informed decisions. The product disclosure sheet should be provided before the cardholder signs up for the debit card-i, and at the point of entering into a contract, if there are material changes in the information. Issuers should also ensure that the product disclosure sheet is made available in Bahasa Malaysia, upon request.

7. PRE-CONTRACTUAL STAGE

7.1 Basic features

7.1.1 Issuers should inform cardholders of the basic features of the debit card-i, including the underlying Shariah contract governing the debit card-i.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 5/26
-----------------	---	---	-----------

7.2 Fees and other charges

7.2.1 Cardholders should be informed of all applicable fees and charges in relation to the debit card-i, including the amount and frequency of payment. The information must be provided in the product disclosure sheet.

7.3 Promotional items

7.3.1 Cardholders should be made aware of the conditions tied to any promotional item and the implications of not complying with such conditions, if any.

8. AT THE POINT OF ENTERING INTO A CONTRACT

8.1 Terms and conditions

8.1.1 Issuers are required to make written terms and conditions for usage of the debit card-i readily available to cardholders. The document should contain a concise but clear description of the major terms and conditions which impose liabilities or obligations on cardholders (in respect of both principal and supplementary cards). Such terms should be described in plain language, which is easily understood by cardholders.

8.1.2 Issuers should advise cardholders to read and understand the terms and conditions before signing the agreement and using the debit card-i. Issuers should take reasonable steps to draw cardholder's attention to the terms that have implications on liability.

8.1.3 Issuers should inform cardholders on the pre-authorisation amount which will be charged to cardholders' accounts when cardholders use the debit card-i at automated fuel dispensers for petrol purchases. Cardholders should also be informed that the issuers may hold the amount up to 3 working days after the transaction date before releasing any extra amount held from the cardholder's account.

8.1.4 Issuers shall ensure that customer service staff are able to answer queries on the debit card-i terms and conditions. The hotlines for the customer service shall be published in the brochures, monthly statements, web pages and at the back of the debit card-i.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 6/26
-----------------	---	---	-----------

8.2 Usage of debit card-i outside Malaysia

8.2.1 Cardholders should be informed of the relevant charges for retail transactions made outside Malaysia.

8.2.2 Cardholders should also be informed of the transaction fees and currency conversion fees applicable on the use of debit card-i for making cash withdrawals overseas.

8.3 Cardholder responsibility

Issuers should highlight to cardholders at the point of entering into a contract, of their responsibilities to:

- a. abide by the terms and conditions for the use of card;
- b. safeguard the card and Personal Identification Number (PIN). Cardholders should be advised not to disclose the PIN or charge card details to anyone;
- c. report lost card / PIN without undue delay;
- d. use the card responsibly, including not using the card for unlawful activity; and
- e. check the monthly statement and report any discrepancy without undue delay.

8.4 Liability for unauthorised transaction

8.4.1 Cardholders should be warned, through clear and prominent notices, of any liability for losses arising from cardholders' failure to notify the issuers immediately after finding that the debit card-i is lost or stolen, or when the cardholders have been found to have acted fraudulently.

8.4.2 Issuers are expected to inform cardholders of the circumstances leading to liability for losses resulting from any unauthorised transaction(s). Cardholders should also be informed of the maximum liability for any unauthorised transaction(s).

8.4.3 Cardholders must be clearly informed of the circumstances in which their liability for loss may exceed the maximum liability for unauthorised transactions to minimise disputes.

8.5 Change of contact details

8.5.1 Cardholders should be informed of the importance of notifying issuers of any change in contact details.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 7/26
-----------------	---	---	--------------

9. DURING THE TERM OF THE CONTRACT

9.1 Statement

- 9.1.1 For any account without a passbook, issuers should provide a monthly statement to cardholders containing information on transaction records and the dates when those amounts were posted to the account.
- 9.1.2 For cardholders that opt to receive e-statements, issuers must ensure that the information on the e-statement is the same as the hardcopy statement.
- 9.1.3 Issuers should maintain on-going efforts to raise cardholders' awareness on measures to prevent debit card-i fraud, including the need to safeguard the card and PIN. The information may be communicated via the monthly statement.

9.2 Closure of account

- 9.2.1 Issuers should allow cardholders to close their debit card-i accounts at any time without being subjected to any fees and charges or a cumbersome account closure procedure.
- 9.2.2 In the event that there is a balance in the debit card-i account, issuers must refund such balance to the cardholder within **30** days from the date of receipt of a closure request.

9.3 Change to the terms and conditions

- 9.3.1 Should there be any change in the terms and conditions, issuers should provide at least 21 calendar days notice to cardholders before the new terms and conditions take effect. Communication to cardholders could be done through monthly statements or other effective means of bringing the charges to the attention of cardholders. The change notice must be prominently displayed.
- 9.3.2 Any change in fees and charges applicable to the debit card-i account should be communicated to cardholders at least 21 calendar days prior to the effective date of implementation.

BNM/RH/CP 008-9	<ul style="list-style-type: none">• Payment Systems Policy Department• Consumer & Market Conduct Department• Islamic Banking and Takaful Department	Concept Paper - Debit Card-i Requirements	Page 8/26
-----------------	---	---	-----------

C. LIABILITY

10. LIABILITY FOR UNAUTHORISED TRANSACTIONS

- 10.1 Issuers shall provide an effective and convenient means by which a cardholder can notify the issuer of any lost, stolen or unauthorised use of his debit card-i and shall implement procedures for acknowledging receipt and verification of the notification of the lost, stolen or unauthorised use of debit card-i.
- 10.2 The cardholder's maximum liability for unauthorised transactions as a consequence of a lost or stolen debit card-i shall be confined to a limit specified by issuers, which shall not exceed RM250, provided the cardholder has not acted fraudulently or has not failed to inform the issuers as soon as reasonably practicable after having found that his card is lost or stolen.
- 10.3 Where the amount imposed on the cardholder for unauthorised transactions due to lost or stolen debit card-i is in excess of the maximum liability limit, the issuer has to prove that the cardholder has acted fraudulently or failed to inform the issuer as soon as reasonably practicable after having found that his debit card-i is lost or stolen.
- 10.4 Cardholders should not be held liable for any unauthorised transactions charged to the debit card-i after the cardholder has notified issuers verbally or in writing, that his debit card-i is lost or stolen. Issuers should have clear processes in place to register any notification of lost/stolen cards and take immediate action upon notification by the cardholder to prevent further use of the lost or stolen debit card-i.
- 10.5 Issuers should inform cardholders in the monthly billing statements of the cardholder's potential liability for unauthorised transactions if he has acted fraudulently or has failed to inform the issuer as soon as reasonably practicable upon discovery of the loss or theft of debit card-i.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 9/26
-----------------	---	---	-----------

D. MARKETING REQUIREMENTS

11. ADVERTISEMENT

- 11.1 Issuers shall ensure that advertisements and promotional materials on debit card-i products are clear, fair and not misleading.
- 11.2 Issuers should establish processes for an independent review of advertisement and promotion materials on debit card-i products, for instance by the Compliance Unit or Legal Unit and Shariah Committee to ensure that they are clear and not misleading.
- 11.3 For print media advertisement, the advertisement should clearly and conspicuously disclose material information about any debit card-i offer that is likely to affect cardholders' decisions. Legible font size should be used to bring cardholders' attention to any important information, relevant fees and charges and eligibility criteria to enjoy the benefits being offered.
- 11.4 Promotion materials should provide adequate information on the key terms and conditions of the debit card-i product. The materials should also contain information on the annual fee and any other applicable charges to facilitate comparisons by cardholders. The information must be presented in plain language and in legible font size.
- 11.5 Issuers should state prominently any important terms and conditions associated with offers of free gifts, prizes, discounts or vouchers for the promotion of debit card-i in print advertisements, or in the marketing materials for new cardholders, or together with the monthly statements for existing cardholders.
- 11.6 In advertising special features or promotions in print media, the applicable eligibility criteria to enjoy the privileges should be disclosed up-front with the announcement. The "applicable eligibility criteria" are those that are imperative to the advertised feature/promotion in addition to the basic terms and conditions of holding the cards. Issuers should not merely indicate in a footnote that "terms and conditions apply".

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 10/26
-----------------	---	---	------------

11.7 Advertisements or other promotion materials should not describe any debit card-i feature as “free” or at “no cost” if other forms of charges will be imposed on cardholders.

12. ISSUER’S OTHER OBLIGATIONS

12.1 Issuers should ensure that sales and customer service representatives (including call centres) are adequately trained and knowledgeable in the key features, benefits and risks of the debit card-i products, including the underlying Shariah contract.

12.2 Issuers should apply due care and diligence when preparing information for use by sales and customer service representatives so that the information is sufficient, accurate, appropriate and comprehensive in substance and form. This is to ensure that cardholders are adequately informed of the terms, benefits and material limitations of the card product or services being offered.

12.3 Issuers should establish procedures and take reasonable steps to ensure that cardholders’ expressed preference (e.g. not to be contacted on new product offers) are duly respected.

12.4 Issuers should put in place adequate verification procedures to confirm the identity of debit card-i applicant to prevent the use of stolen information (e.g identity theft) for debit card-i applications.

E. OTHER REQUIREMENTS

13. CUSTOMER INFORMATION

13.1 Issuers are required to comply with the requirements on disclosure of customer information as specified under section 10 (under general policy requirements) of the Guidelines on Products Transparency and Disclosure.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 11/26
-----------------	---	---	------------

14. COMPLAINTS MANAGEMENT

- 14.1 Issuers are required to comply with the complaints management requirements as specified in the “Guidelines on Complaints Handling” issued by Bank Negara Malaysia.
- 14.2 Issuers should provide cardholders with information on how complaints may be made and the contact details of the issuer’s complaints unit. In addition, contact details of BNM LINK and BNMTELELINK should be provided in the monthly debit card-i statement.

15. USAGE OF DEBIT CARD-i FOR UNLAWFUL ACTIVITIES

- 15.1 Issuers shall include in the terms and conditions a clause specifying that the debit card-i are not to be used for any unlawful activities.¹ Issuers shall immediately terminate the debit card-i facility if the cardholder is found to have used the debit card-i for an unlawful activity.

PART 2

F. RISK MANAGEMENT

The rapid pace of technological innovations has changed the scope, complexity and magnitude of risks that issuers and acquirers face in carrying out the debit card-i business. Issuers and acquirers are expected to have adequate processes and controls in place to manage and respond to such risks, including operational risk associated with debit card-i business.

16. EFFECTIVE MANAGEMENT OVERSIGHT

- 16.1 The Board of Directors and senior management of issuers and acquirers shall establish effective management oversight over the risks associated with their debit card-i operations, which include, among others, the following:
- 16.1.1 Establishment of a comprehensive risk management process and internal

¹ For example, illegal online betting.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 12/26
-----------------	---	---	------------

controls for managing and monitoring risks associated with their debit card-i operations.

- 16.1.2 Establishment of processes for the review, approval and implementation of appropriate policies and procedures governing the debit card-i operations to ensure the risks in their debit card-i operations are adequately mitigated.
- 16.1.3 Oversight of the development and continued maintenance of the security infrastructure that safeguards their debit card-i systems and data from internal and external threats.
- 16.1.4 Audit by an independent party should be required and undertaken with reasonable frequency to ascertain and detect weaknesses in the entire card process in a timely manner.
- 16.1.5 Establishment of a comprehensive and ongoing due diligence and oversight process to manage outsourced arrangements and other third-party dependencies supporting the debit card-i operations.

16.2 The Board of Directors and senior management of issuers and acquirers shall also ensure that a strong management information system (MIS) is in place to support decision making, analysis and risk management.

17. COMPREHENSIVE SECURITY POLICIES, PROCEDURES AND CONTROLS

Issuers and acquirers shall implement and enforce relevant policies and procedures to ensure confidentiality, integrity and availability of data as well as to ensure the system and network infrastructure are safe and secure.

- 17.1 Robust security controls such as firewall, intrusion detection and prevention systems, etc. shall be put in place to secure the system and network infrastructure while penetration tests shall be performed regularly.
- 17.2 Procedural and administrative controls on critical processes shall be put in place. Critical processes include, but are not limited to, the following:
 - 17.2.1 PIN generation and printing

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 13/26
-----------------	---	---	------------

PIN generation and printing processes are tasks that should be performed in a highly secure environment. In this regard, the following shall, at the minimum, be observed:

- a. Usage of hardware-based PIN generation and verification.
- b. Generated PINs shall be protected from being accessed or viewed by unauthorised persons.
- c. The process of generating the PIN has to be strictly controlled. PIN generation and printing area should be strictly restricted to authorised personnel only.
- d. Regeneration of same PIN for same card/account shall be prohibited.
- e. At least one independent party (which may be personnel independent of the process) shall be present to observe and check that the processes are in accordance to accepted procedures.

17.2.2 Personalisation² process

- a. Personalisation process shall be performed in a secure environment. Access to personalisation machine, reader and data shall be strictly restricted.
- b. Data used for personalisation shall be classified as confidential information and issuers shall ensure confidentiality and safety of the data that has been sent, stored and processed. These data shall be deleted upon completion of the process.
- c. Sensitive keys used to perform personalisation shall be kept in a secure manner. Adequate policy and procedures to govern the management of such keys shall be put in place.
- d. Periodic card inventory reconciliation and audit shall be performed on blank cards.
- e. Card personalisation centre shall ensure that the following controls are in place:
 - i. Adequate physical and logical security controls.
 - ii. Segregation of duties and dual control.
 - iii. Network security control.

² A process of injecting/encoding customer data into the blank card's chip/magstripe; and embossing the cards with customer's details e.g. name, expiry date, etc.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 14/26
-----------------	---	---	---------------

When the card personalisation process is outsourced, controls shall be in place to ensure that data sent for personalisation to outsourced parties are secured. The issuers must monitor the outsourced vendor to ensure that the above requirements are met.

- 17.3 Effective segregation of functions on handling of debit card-i and PIN shall be observed at all stages of processing, particularly the following:
- 17.3.1 Card processing (e.g. embossing and encoding processes) and PIN generation functions.
 - 17.3.2 Physical management of card and PIN including mailing (if applicable).
- 17.4 Effective dual control over critical functions shall be implemented. Critical functions include the following:
- 17.4.1 Setting and maintaining all system parameters.
 - 17.4.2 PIN generation processes and handling of secret keys or codes and other unique security features.
 - 17.4.3 Handling and safekeeping of blank cards.
 - 17.4.4 Handling of returned and undelivered debit card-i.
- 17.5 Necessary measures shall be taken to ensure the confidentiality of debit card-i data and information.
- 17.5.1 Confidential data and sensitive information shall be protected from unauthorised viewing or modification during transmission and storage.
 - 17.5.2 Sensitive information shall be encrypted end to end during transmission over the network.
 - 17.5.3 Minimal account information shall be printed on sales draft to minimise the risk of misuse of information to conduct fraudulent “card-not-present” transactions.
 - 17.5.4 Storage of sensitive authentication data, e.g. magnetic stripe data, PIN and validation code (e.g. three digit numbers on debit card-i used to verify card-not-present transactions) should not be allowed as this information may be used by fraudsters to generate fake debit card-i and create fraudulent transactions.
 - 17.5.5 Confidential data and sensitive information shall only be accessible and

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 15/26
-----------------	---	---	------------

managed by authorised parties.

- 17.6 Proper identification and authentication method (e.g. passwords and PINs) shall be adopted to avoid unauthorised usage of debit card-i as well as unauthorised access to system, network and data. For more robust security, the following shall be adopted at the minimum:
- 17.6.1 PIN shall be at least six digits in length. Password shall be alphanumeric and at least six characters in length. Where possible, the use of strong PIN/password shall be adopted.
 - 17.6.2 Maximum PIN/password tries shall be limited to three on an accumulated basis.
 - 17.6.3 PIN shall not be stored permanently in any format or media. Passwords should be securely maintained.
 - 17.6.4 If the PIN/password is computer-generated and is not chosen by the cardholder, mandatory PIN/password change shall be adopted before the first transaction is permitted.
 - 17.6.5 Cardholders shall be allowed to change the PIN/password at any time.
- 17.7 Disposal of debit card-i related materials/assets, such as damaged or returned cards, reports, embossing machines, etc., shall be performed in a controlled environment.

18. ROBUST OPERATIONAL RELIABILITY AND BUSINESS CONTINUITY

A high level of system availability is required to maintain public confidence. Issuers and acquirers should ensure that they have the resources and capacity in terms of hardware, software and other operating capabilities to deliver consistently reliable and secure services.

- 18.1 Measures to ensure operational reliability include, but are not limited to, the following:
- 18.1.1 Strong internal controls for system and personnel administration.
 - 18.1.2 Comprehensive and well-documented operational and technical procedures to ensure operational reliability.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 16/26
-----------------	---	---	------------

18.1.3 Sufficient capacity of the system to support business requirements.

18.1.4 A robust business continuity and disaster recovery plan, including a highly reliable backup system.

19. OUTSOURCING RISK MANAGEMENT

Outsourcing does not reduce the fundamental risk associated with debit card-i operations. Neither does it absolve the issuers and acquirers from their responsibilities of having to manage the risks of their debit card-i operations. As such, issuers and acquirers that outsource any part of their debit card-i operations shall observe the minimum requirements set out below.

19.1 Prior to entering into any outsourcing arrangement, the following should, at the minimum, be considered:

19.1.1 Availability of sufficient expertise within the issuer/acquirer to oversee and manage the outsourcing relationship.

19.1.2 Scope and critical nature of services/operations to be outsourced.

19.2 Issuers and acquirers should also perform appropriate due diligence review of the integrity, competency and financial viability of the outsourcing service provider before the arrangements are formalised.

19.3 The outsourcing agreement should be comprehensive and include the following:

19.3.1 Clearly defined roles, responsibilities and obligations of the service provider.

19.3.2 Clear provisions for Bank Negara Malaysia to enter the premises of the service provider to conduct examination and investigation with regard to the services outsourced, should the need arise.

19.3.3 Conditions under which the outsourcing arrangement may be terminated.

19.4 Although the operational activities of debit card-i are outsourced, reporting and monitoring mechanisms should be put in place by issuers and acquirers to ensure that the integrity and quality of work conducted by the outsourced service provider is maintained.

19.5 Regular due diligence should be conducted on the outsourcing service provider and

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 17/26
-----------------	---	---	------------

periodically reviewed to ensure the suitability and performance of the service providers.

- 19.6 Periodic independent internal and/or external audits should be conducted on the outsourced operations with at least the same scope as if the operations had been conducted in-house.

20. FRAUD RISK MANAGEMENT

Issuers and acquirers need to be vigilant of the evolving typologies of fraud and monitor such developments on an on-going basis.

- 20.1 Issuers and acquirers shall deploy effective and efficient fraud detection and monitoring mechanism.

20.1.1 The fraud detection and monitoring of transactions should be conducted on an on-line real time basis.

20.1.2 The fraud detection and monitoring mechanism should be able to capture high risk transactions and trigger unusual transactions.

a. Issuers shall put in place criteria for high risk transactions and merchants to facilitate early detection of fraud.

b. Issuers shall put in place procedures to facilitate early detection of unusual transaction pattern or trend that could be indicative of fraud and take necessary action to block/delay these transactions for further investigation.

- 20.2 Issuers and acquirers shall establish comprehensive fraud investigation, analysis and reporting procedures.

20.2.1 Issuers and acquirers shall conduct regular analysis to understand the fraud trend and modus operandi.

20.2.2 Adequate risk management processes, systems and controls shall be in place, and where necessary, strengthened, to mitigate fraud risk taking into account new developments in fraud trends and material changes in the business strategy which may increase exposure to potential fraud risk.

20.2.3 Fraud incidents shall be reported to senior management and the Board on

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 18/26
-----------------	---	---	------------

a regular basis. Reporting to Bank Negara Malaysia shall be in accordance to the fraud reporting requirement imposed by Bank Negara Malaysia from time to time.

Fraud prevention mechanism

Fraud may take place during the course of the different cycles of the entire debit card-i value chain, i.e. card application, card delivery, card activation, change of cardholder's contact details as well as when the card is in the possession or being used by the cardholder.

Minimum Fraud Mitigation Measures for Card Application, Delivery and Activation

20.3 The following shall be observed at the point of collecting card applications from applicants:

20.3.1 Issuers shall ensure the confidentiality of the data and information provided by the applicant. Necessary measures should be put in place to ensure that the information provided by the applicant would not be misused by the persons authorised by the issuer to collect the application(s).

20.3.2 Issuers or any persons acting on behalf of the issuers to collect card applications are prohibited from photocopying the applicants' other debit card-i. This is because card security features which are used for cardholder authentication are available on the card itself such as card number, Card Verification Value (CVV) and expiry date of the card.

20.4 The following controls shall be taken into consideration when processing card applications:

20.4.1 The identity of the applicant should be verified to ensure that the applicant exists and is the person applying for the card.

20.4.2 Key information provided by the applicant should be verified for accuracy.

20.4.3 Issuers should ensure the confidentiality of the data and information provided by the applicant.

20.5 Issuers are prohibited from sending out live cards to its cardholders. Stringent activation procedures, which shall include proper verification process that cannot be easily bypassed by fraudsters including its own employees, should be implemented

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 19/26
-----------------	---	---	------------

unless the cards are personally collected by the cardholder from the issuers' premises and subjected to proper verification process.

Requirements when Changing Cardholder's Contact Details

20.6 To mitigate the risk of account takeover, issuers shall put in place measures to verify any request it received for change of address and shipment of new or replacement card or PIN. Some examples of best practices that the issuers may consider include:

20.6.1 Allow request only if it is made in person at the issuer's premises.

20.6.2 Allow request through secured electronic mode (e.g. electronic banking) but subject to further verification before updating the contact details.

20.6.3 Send written correspondence to the previous address for verification before shipping any card or PIN to the new address.

Implementation of "Chip and PIN" technology

20.7 In line with efforts to enhance the security features of debit card-i, all issuers and acquirers are required to enable chip and PIN verification for debit card-i transactions at point-of-sale terminals (POS) and cash withdrawals at automated teller machines (ATMs).

Implementation of strong authentication method for non face-to-face transactions

20.8 Non face-to-face transactions, i.e. card-not-present transactions, especially online payments, are currently the main modus operandi for fraud globally. This is due to the vulnerability posed by this type of transaction whereby cardholders need not be personally present to have the transaction completed.

20.9 Issuers and acquirers are required to implement measures to authenticate cardholders for online transactions. Issuers are required to adopt strong authentication method, such as dynamic password/PIN, multi-factor authentication (e.g. mobile PKI), etc., to mitigate the risk of unauthorised use of cards for online transactions.

Implementation of transaction alerts

20.10 Issuers are required to implement transaction alerts via short message service

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 20/26
-----------------	---	---	------------

(SMS) to their cardholders, unless cardholders opt to receive transaction alerts via other channel such as e-mail. This shall be applicable to the following:

- 20.10.1 Purchase transactions at POS.
- 20.10.2 Online transactions.
- 20.10.3 Cash withdrawal transactions.
- 20.10.4 Mail and telephone order transactions.

20.11 Issuers are required to take into consideration the following minimum criteria to trigger transaction alerts:

- 20.11.1 Transaction type, e.g. transaction at high risk merchants³.
- 20.11.2 Transaction location, e.g. transaction in high risk countries⁴.
- 20.11.3 Transaction amount, e.g. transaction exceeding certain amount.
- 20.11.4 Transaction velocity, e.g. transaction exceeding certain number per day.
- 20.11.5 First time use of new card.

20.12 Issuers **are required** to send transaction alerts in the event any of the following trigger is met:

- 20.12.1 Transactions exceeding a specified threshold amount. In this regard, issuers are required to set a threshold amount to trigger an alert. Issuers should also allow cardholders to set their own preferred threshold amount for the transaction alert. If cardholders do not set the preferred threshold amount, issuers are required to send transaction alerts based on the default threshold amount set by the issuer.
- 20.12.2 First time use of new card.
- 20.12.3 All card-not-present transactions.
 - a. Issuers are not required to send transaction alerts for auto-debit transactions. However, issuers should take the necessary steps to ensure the auto-debit transaction is a genuine transaction and disputes, if any, are handled appropriately so that cardholders are sufficiently safeguarded.

20.13 By default, the alert should be sent for transactions meeting the specified criteria, except where the cardholders opt not to receive any SMS alerts. In this regard,

³ Minimum list of high risk merchants will be specified by the industry.

⁴ Minimum list of high risk countries will be specified by the industry.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 21/26
-----------------	---	---	------------

issuers should ensure that the cardholders:

- 20.13.1 understand the risks associated with their decision; and
- 20.13.2 submit such request in writing.

20.14 To ensure the effectiveness of the alerts, issuers should ensure that the contact numbers of their cardholders are kept up-to-date. As such, issuers should highlight to their cardholders the criticality of providing updated contact numbers to them.

20.15 To mitigate abuse, issuers shall not provide a contact number as part of the message in the SMS alert. Instead, issuers should advise cardholders to contact their card centre and use the contact number indicated at the back of their debit card-i.

20.16 Issuers shall not transfer the cost of sending SMS alerts to their cardholders.

20.17 Issuers may stop sending transaction alert for purchase transactions at POS and cash withdrawal transactions after full implementation of chip and PIN technology, and for online transactions after adoption of strong authentication method.

Exchange of information and dissemination

20.18 Sharing of information regarding fraud experiences and modus operandi is encouraged among issuers and acquirers as this will enhance efforts to combat fraud.

20.19 Issuers and acquirers should also be resourceful in gathering relevant information from the industry, their overseas counterparts, the card associations, etc. Having first hand information will assist them to strengthen their defence against fraudsters.

20.20 Close cooperation with law enforcers and regulators should also be established.

21. SPECIFIC REQUIREMENTS FOR ACQUIRERS

Acquirers should be diligent in their acquiring business to ensure that they are not being used by the merchants as a means to easily obtain funds through illegal means, fraudulent

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 22/26
-----------------	---	---	------------

acts or cheating. Controls should be put in place both prior to engaging the merchant and on an ongoing basis.

21.1 Acquirers should establish the criteria for merchant selection and recruitment, and establish policies and procedures for ongoing monitoring of their merchant accounts, which should include risk criteria for merchants.

Merchant recruitment

21.2 Acquirers shall establish prudent underwriting criteria and procedures for approving new merchants. The criteria for assessing new merchants should also cover financial strength and reputation (e.g. has not been declared a bankrupt, has a clean fraud track record, has not been blacklisted by other acquirers etc.).

21.3 Acquirers should ensure that the merchant has a legitimate business and is not involved in or otherwise associated with any illegal activities or schemes, including business activities that are meant to deceive consumers, such as schemes like “scratch and win”, “get-rich-quick”, etc.

21.4 If a third party merchant recruitment agent is engaged, acquirers shall ensure proper controls are in place to ensure that the third party merchant recruitment agent complies with relevant requirements issued by Bank Negara Malaysia.

Merchant monitoring and audit

21.5 Acquirers should monitor the trend in chargebacks and merchant’s capacity to repay these chargebacks and act accordingly to mitigate any risks associated with engaging such merchants.

21.6 Acquirers shall take appropriate risk management measures on their high risk merchants, including conducting more frequent audit/checks on the merchant and more stringent monitoring of transactions that pass through the merchant.

21.7 The relationship with merchants with confirmed fraudulent or illegal activity should be immediately terminated. Whenever the merchant has been terminated or blacklisted due to fraud-related matters by one of the acquirers, other acquirers shall be vigilant and gather relevant information and evidence on the conduct of the said merchant.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 23/26
-----------------	---	---	------------

- 21.8 Acquirers shall conduct continuous due diligence on their merchants to ensure that merchants are not involved in any fraudulent or illegal activity and maintain a “watch list” of suspected collusive merchants, if any. The activities of these merchants shall be closely monitored and investigated. Once identified as collusive, acquirers shall immediately terminate their acquiring relationship with the merchant.
- 21.9 Acquirers shall conduct periodic audits on the merchants to ensure that merchants adhere to card acceptance and authorisation procedures to minimise chargeback and disputes.

22. COMPLIANCE WITH OTHER REQUIREMENTS

- 22.1 Issuers shall comply with other relevant guidelines or requirements issued by Bank Negara Malaysia from time to time.

G. APPROVED SHARIAH CONCEPT APPLIED IN DEBIT CARD-i

23. SHARIAH CONCEPT

- 23.1 The underlying Shariah concept that may be applied in debit card-i is *ujrah* (fee). Under this concept, *ujrah* (fee) will be charged to customer in consideration of identified services, benefits and privileges. Such services may include payment facility for goods and services; and cash withdrawal from customer’s account via automated teller machine.

General Conditions for Debit Card-i Facility

- 23.2 The issuance of debit card-i by the issuer to cardholder and the use of the aforesaid card shall be subject to the terms and conditions made known to the cardholder. Necessary arrangement shall be made such as obtaining consent from contracting parties prior to any action made which is against the agreed terms and conditions.
- 23.3 The issuer and the cardholders shall ensure that the debit card-i is not used for non-Shariah compliant transaction.

BNM/RH/CP 008-9	<ul style="list-style-type: none">• Payment Systems Policy Department• Consumer & Market Conduct Department• Islamic Banking and Takaful Department	Concept Paper - Debit Card-i Requirements	Page 24/26
------------------------	--	--	-------------------

23.4 Any privileges granted by card issuer shall only include services and benefits that are in compliance with Shariah.

23.5 The acquirer shall ensure that the contract with the merchant is Shariah compliant.

23.6 The fee shall only be charged on services, benefits and privileges provided.

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 25/26
-----------------	---	---	------------

APPENDICES

Appendix 1 Product Disclosure Sheet – Debit Card-i

<p>PRODUCT DISCLOSURE SHEET</p> <p>(Read this Product Disclosure Sheet before you decide to take out the <Name of Product>. Be sure to also read the general terms and conditions.)</p>	<p><Name of Financial Service Provider></p> <p><Name of Product></p> <p><Date></p>
<p>1. What is this product about?</p>	
<p>This is a debit card-i, a payment instrument which allows you to pay for goods and services from your deposit account at participating retail and service outlets. You are required to maintain a deposit account with us, to be linked to your debit card-i. If you close your deposit account maintained with us, your debit card-i will be automatically cancelled.</p>	
<p>2. What are the fees and charges I have to pay?</p>	
<ul style="list-style-type: none"> • Annual fee • Domestic ATM withdrawal fee • Overseas transaction conversion fee • Card replacement fee • Sales draft retrieval fee • Additional statement request fee • Others 	
<p>3. What are the key term and conditions?</p>	
<ul style="list-style-type: none"> • Pre-authorization for payment using debit card-i Pre-authorization amount of RMXXX will be charged to your payment instrument account / banking account when you make payment using your debit card-i at automated fuel dispenser. We will only post the exact amount of transaction and release any extra hold amount from your account within 3 working days after the transaction date. 	
<p>4. What if I fail to fulfil my obligations?</p>	
<ul style="list-style-type: none"> • Your liability for unauthorised transactions. <i>(To highlight other key terms and conditions.)</i> 	
<p>5. What are the major risks?</p>	
<p>Your card being stolen or lost. You should notify us immediately after having found that your debit card-i is lost or stolen.</p>	

BNM/RH/CP 008-9	<ul style="list-style-type: none"> • Payment Systems Policy Department • Consumer & Market Conduct Department • Islamic Banking and Takaful Department 	Concept Paper - Debit Card-i Requirements	Page 26/26
-----------------	---	---	------------

6. What do I need to do if there are changes to my contact details?

It is important that you inform us of any change in your contact details to ensure that all correspondences reach you in a timely manner.

7. Where can I get further information?

If you have any enquiries, please contact us at:

ABC Bank Berhad
51, Jalan Sultan Ismail
50122 Kuala Lumpur
Tel:
Fax:
E-mail:

8. Other debit card-i packages available

- abc
- xyz

The information provided in this disclosure sheet is valid as at dd/mm/yy.