June 2006

Stored Value Facility Guidelines

Monetary Authority of Singapore

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 OVERVIEW

1.1.1 A stored value facility ("SVF") is a facility that is used for payment of goods or services up to its stored value. A person who wishes to use an SVF ("user") will purchase the SVF containing a certain stored value. This stored value amount is paid in advance to the stored value holder of a SVF ("holder"). Thereafter, the user will be able to use the SVF to purchase goods or services from merchants who accept the stored value in the SVF as payment ("merchants"). These merchants will redeem from the holder the stored value that they have accepted from users. SVFs can be provided in different forms, such as smart cards, contact-less cards, magnetic stripe cards, paper vouchers, micro-chips and internet accounts. Certain forms of SVFs allow for the "topping up" of additional stored value in consideration of cash or other means of payment.

1.1.2 The holder plays an important role in ensuring the safety and efficiency of the SVF. If the holder is unable to meet its obligations to users or merchants, both users and merchants may be inconvenienced or even financially affected, thereby leading to a loss of confidence in the SVF. This could occur when there is a disruption in the SVF operation, or when the holder has not prudently managed the money collected from users.

1.1.3 These Guidelines recommend sound principles and risk mitigating measures for the operation of a SVF. They address important issues, such as transparency, disclosure, public confidence, stored value protection, prevention of money laundering and countering the financing of terrorism. By issuing these Guidelines, the Monetary Authority of Singapore ("MAS") aims to advance the safety and soundness of SVFs and promote user confidence.

1.2 Definitions and Generic Model of SVF

1.2.1 SVFs may differ in terms of technical implementation and business structure. The relationship of the major stakeholders in a typical SVF is illustrated in Figure 1. The terminologies used in these Guidelines are:

- **User:** A person who purchases the SVF and uses it as a means of making payment for goods or services.

- **Holder:** A person who holds the money that the user pays to acquire stored value in the SVF. The holder makes payment to merchants who have provided goods or services to the user.

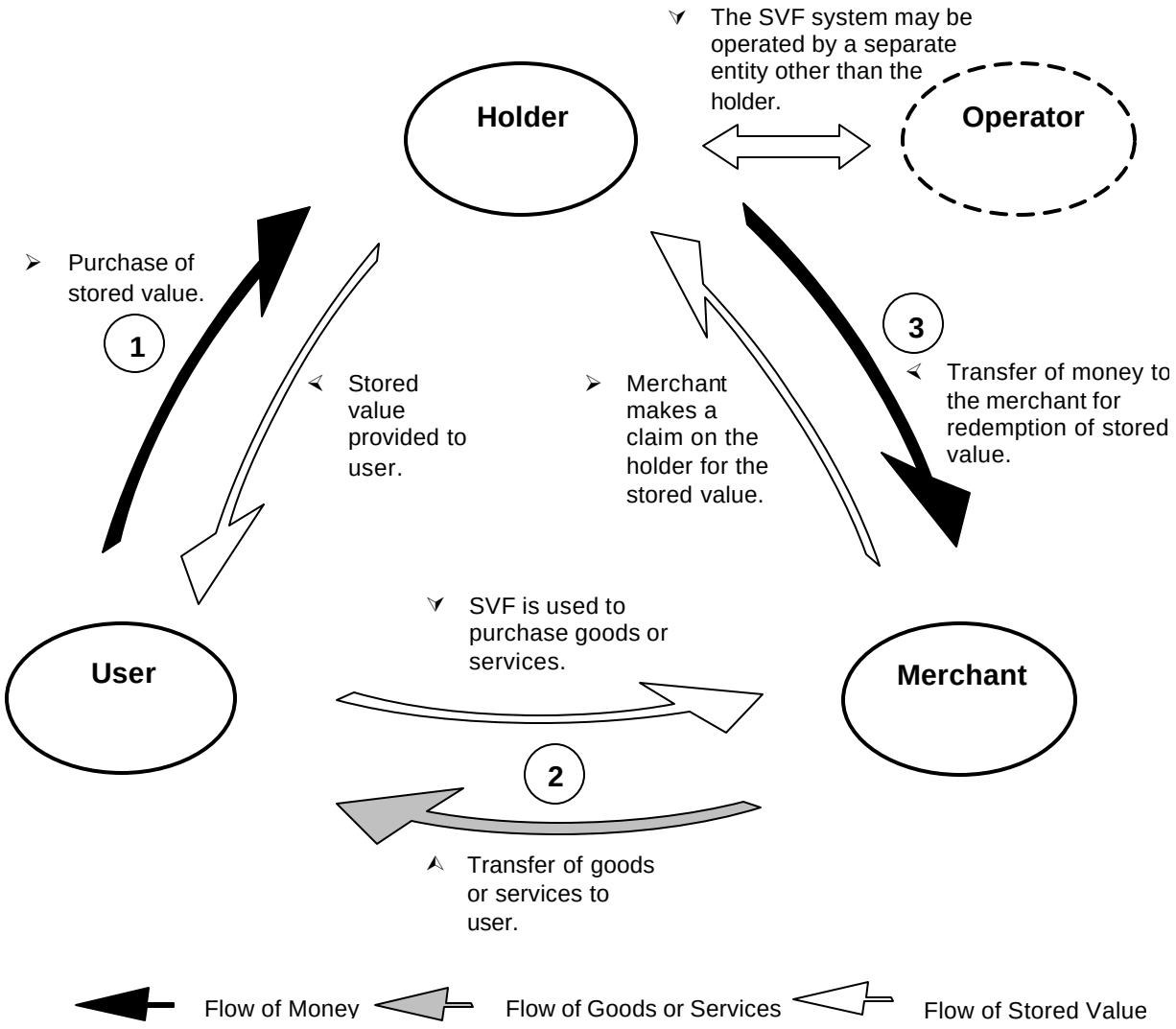
- **Operator:** A person who operates the payment system in respect of the SVF. A holder may be the operator of the SVF.

- **Merchant:** A person, including the holder, who accepts the SVF as a means of payment and provides goods or services in exchange. The merchant will make a claim on the holder for the stored value it has accepted from users.

1.2.2 The above four stakeholders interact through three core flows in a standard SVF as illustrated in Figure 1:

1. The user purchases an amount of stored value in the SVF;
2. The user redeems the stored value via the purchase of goods or services from merchants that accept the SVF; and
3. The holder reimburses the merchant for the stored value collected from funds provided by the user.

Figure 1: Flow of money and stored value for a standard SVF



1.3 Applicability of the Guidelines

1.3.1 Before establishing a SVF, a prospective holder should undertake its own due diligence to ensure that the intended SVF will comply with all relevant laws and regulations. In particular, the prospective holder should ensure compliance with the Payment Systems (Oversight) Act 2006 ("PS(O)A") and related regulations.

1.3.2 The Guidelines recommend sound principles and practices, including the implementation of sound processes for the issuance and operation of a SVF. Holders are strongly encouraged to adopt and implement the Guidelines, taking into consideration the nature, size and complexity of their SVFs.

1.3.3 For widely-accepted SVFs, as defined under the PS(O)A, the principles and practices in these Guidelines will serve as minimum standards.

2.0 PRINCIPLES

2.1 PRINCIPLE 1: HOLDERS SHOULD PROVIDE FOR A TIMELY REDEMPTION OF STORED VALUE IN THE SVFS.

2.1.1 Upon acquiring stored value in respect of a SVF a user should be able to redeem the stored value in two ways. Firstly, the user should be able to redeem the stored value in the SVF in exchange for goods or services from merchants. Secondly, the user should be able to obtain a refund from the holder in respect of the stored value in an SVF.

2.1.2 Refunds should be allowed unless the holder is able to prove that the SVF is a counterfeit, the stored value in the SVF has been illegally updated, or the stored value has not been updated in accordance with the procedure stated in the terms and conditions ("T&Cs") governing the use of the SVF. Upon receiving a claim for the refund of the balance value in the SVF, the holder should provide the full refund of the unused stored value either in cash, cheque or by crediting a bank account designated by the user.

2.1.3 The T&Cs governing the use of the SVF should include refund procedures, and, if any, the time limit for refunds, administration fee for refunds and expiry period of the stored value.

Timely redemption

2.1.4 In order to meet users' redemption of stored value in a timely manner, a holder should have sufficient assets to meet the full redemption of the total stored value. On a daily basis, the holder should maintain an amount of cash and liquid assets which is commensurate with the redemption patterns or projected redemption patterns of the SVF. The redemption patterns should be monitored closely to ensure that the necessary liquidity is available. The holder should make reasonable provisions for possible increases in redemption on certain days. For example, the use of the SVF may increase when a significant new merchant participates in the SVF. There may also be an increase in redemption as a batch of SVFs approaches the expiry date.

2.1.5 The holder should ensure that a user is able to receive a timely refund of the stored value when the user presents the SVF for refund. The holder should provide users with access to proper refund facilities. For example, the refund facilities should be accessible at least during office hours.

If the refund facilities are physical, they should be made available at convenient locations.

2.1.6 In the event of any disruption in the normal operations of the refund facilities, such as arising from system disruption or failure, the holder should make available to users contingent refund arrangements within seven days from the occurrence of the event. Within forty-eight hours of the disruption, the holder should notify users of the contingent arrangements that will be made available. Where appropriate, the holder should inform users of such contingent arrangements through the publication of prominent statements in the media. The ability to recover expeditiously from a major disruption will help preserve the SVF's reputation and maintain user confidence.

Stored value preservation

2.1.7 The holder should exercise prudence in the management of the stored value so that the ability to provide timely redemptions by users is not impaired. To minimise the risk of mishandling, it is recommended that the holder deposit the stored value in a designated bank account separate from working capital funds, or place the stored value in a bank account held on trust for users.

2.1.8 If the holder chooses to invest the stored value, it should invest in liquid and low-risk assets, such as fixed deposits or government treasury bills to ensure capital preservation. Higher risk investment strategies that could diminish the stored value should be avoided.

2.2 PRINCIPLE 2: HOLDERS SHOULD ENSURE THAT THEIR SVFS OPERATE IN A SECURE AND RELIABLE MANNER.

2.2.1 A holder's primary responsibility to users is to meet users' redemptions. The holder should have in place adequate policies, procedures and systems for its SVF operations, including contingency plans to address operational disruptions.

Operational risk

2.2.2 Operational risk refers to the risk of direct or indirect loss resulting from inadequate or failed internal processes and systems. Holders should implement operational and security safeguards which are commensurate with the scale and complexity of their SVFs. For example, a firewall system should be put in place to safeguard an SVF which involves the use of the Internet, while anti-counterfeiting measures may be required to safeguard a physical SVF. Examples of risk mitigating measures that holders may adopt include, but are not limited to:

- Robust system design, development, testing, implementation and monitoring;
- Strong internal controls for systems and personnel administration;
- Comprehensive operating control policies and procedures;
- Regular independent checks on systems and processes by security professionals or internal auditors; and
- Robust business continuity plans, which should include backup and recovery of SVF databases.

Security risk

2.2.3 Security risks need to be appropriately addressed, especially for a SVF that is heavily dependent on electronic or network systems. Security vulnerabilities in these systems can pose a significant threat to the integrity of the SVF. Inadequate management of security vulnerabilities may give rise to the risk of fraud, such as counterfeiting. If counterfeit stored values are introduced into the SVF and redeemed, the available funds will fall short of legitimate claims against the holder.

2.2.4 A holder should mitigate security risks through the implementation of a safe and robust security risk management framework that will be able to actively identify, assess, reduce and monitor security risk. Risk-monitoring

features should be in place to ensure that systems are operating at the predefined levels of reliability and security. MAS Internet Banking Technology Risk Management Guidelines provide additional guidance on security risk framework, which may be relevant for technologically dependent and large-scale SVFs. The security risk framework established by the holder should address the following:

- Data confidentiality;
- System and data integrity;
- Authentication and non-repudiation;
- System availability; and
- Customer protection.

2.2.5 A holder may provide mobile payment services to enable users to make payments, top-up or redeem stored value. The risks associated with the use of mobile technology vary with the type of services offered and the value of transactions in such services. Other factors that affect the risks involved are the devices used, the delivery channels chosen, and the systems which process the mobile transactions and enable the interaction between the holder, users and merchants. MAS Security Guidelines for Mobile Banking & Payments provide guidance on the management of these risks.

Outsourcing risk

2.2.6 A holder may outsource the operational activities of its SVF to another party. However, outsourcing cannot relieve the holder from its obligations to users. The holder should carry out regular due diligence on every outsourcing service provider and periodically review the suitability and performance of the service providers. The risk management practices that the holder may apply include, but are not limited to:

- Systematic risk evaluation framework;
- Comprehensive outsourcing agreement and assessment of service provider capability;
- Robust confidentiality and security procedures and controls; and
- Sound business continuity management.

2.3 PRINCIPLE 3: HOLDERS SHOULD ENSURE THAT THE RIGHTS AND RESPONSIBILITIES OF ALL STAKEHOLDERS OF THE SVFS ARE FAIR AND CLEARLY DEFINED.

2.3.1 A holder must ensure that the rights and obligations of all stakeholders (e.g. users and merchants) of the SVF are clearly set out in the relevant contractual documents, and the interests of all stakeholders are fairly considered in the construction of the legal arrangements. These arrangements include, but are not limited to:

- Associated fees and charges payable by users or merchants relating to services provided by the operator and holder of the SVF;
- Liability of each stakeholder in loss events, such as financial or operational failure of the holder or operator, fraud, counterfeiting and theft of the stored value;
- Coverage of stored value held by the holder under protection agreements, such as insurance, banker's guarantee or trust;
- Dispute resolution arrangements, including the dispute resolution mechanism and the applicable rules and procedures;
- Replacement policy regarding loss, theft or malfunctioning of SVFs;
- Users' right to obtain refund of unused stored value; and
- Validity and expiry clauses, such as treatment, claim periods, and receipt of unclaimed and expired stored value amount.

2.4 PRINCIPLE 4: HOLDERS SHOULD PROVIDE ADEQUATE DISCLOSURE OF USERS' RIGHTS AND OBLIGATIONS.

2.4.1 The agreement between a user and a holder or user, holder and operator should be easily accessible and understood by the users. The holder should ensure that users are informed and updated on their full rights and responsibilities under the agreement. The agreement should also clearly state the holder's role and responsibilities. Further, the holder should ensure that users are provided with other relevant information relating to the usage of the SVF.

2.4.2 The holder should provide every user with a copy of the agreement upon the user's purchase of the SVF and upon any subsequent request. The agreement should be printed in clear and legible type, and be of a readable font size. If it is not practical to provide a physical copy of the agreement at

the point-of-sale, the holder should prominently provide directions on how to obtain the agreement. For example, the holder may direct the user to its website to obtain a copy of the agreement.

2.4.3 For any significant change to the SVF, such as a change in the T&Cs governing the use of the SVF or a change in holder, the holder should ensure that users are given sufficient notice prior to the change. The holder should choose an appropriate medium to announce the changes to all current and potential users in a manner that does not unduly rely on the users' own initiative. An example is the use of local mass media.

2.4.4 Users should be able to easily identify the holder of a SVF. For example, where the SVF is physical in nature, the holder's identity should be clearly stated on the SVF.

2.5 PRINCIPLE 5: HOLDERS SHOULD IMPLEMENT ADEQUATE MEASURES TO PREVENT THE USE OF SVFS FOR MONEY LAUNDERING AND TERRORIST FINANCING.

2.5.1 SVFs provide transacting parties with immediate, convenient and potentially anonymous means to transfer financial value. The convenience and anonymity of SVF transactions may make SVFs attractive vehicles for money laundering and terrorist financing activities. Hence, a holder should consider designing and implementing a SVF that reduces opportunities and incentives for such abuse and provides the means to filter out suspicious activities.

2.5.2 A holder should ensure that its SVF complies with all relevant laws and regulations pertaining to money laundering and terrorist financing, in particular the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 84A), and Terrorism (Suppression Of Financing) Act (Cap. 325).

2.5.3 In order to prevent and detect money laundering in SVFs, measures that should be undertaken by a holder include, but are not limited to:

- The load limit[1] for any SVF should not exceed S$1,000[2]. A lower load limit for an unregistered SVF[3] should be considered;
- Bulk purchases of any SVF should be capped at S$20,000 per transaction. For example, if a holder in respect of a SVF loads its SVFs with S$1,000, it can only sell up to 20 such SVFs to any user at any one time;
- Stored value should not be transferable between unregistered SVFs. Stored value should only be redeemed at a merchant in exchange for goods or services, or refunded by the holder;
- Audit trails should be incorporated in the SVF so that the holder can assist relevant authorities to identify unusual transaction patterns and help trace any person who uses the SVF to carry out illegal activities; and
- Policies and procedures should be implemented by the holder to identify and report suspicious activities as part of its on-going surveillance. This can be achieved by monitoring the use of the SVF to track any unusual or suspicious transaction.

[1] The load limit is the maximum amount of stored value an SVF can hold at any one time.

[2] The S$1,000 load limit represents a balance between user freedom and the risk of money laundering and terrorist financing.

[3] An unregistered SVF is one that does not require any record to be made of the user.

3.0 CHECKLIST

The checklist summarises the key sound practices and risk mitigation measures for the operation of a SVF and is not meant to be exhaustive. SVF holders should refer to the Guidelines for further elaboration.

Principle 1: Holders should provide for a timely redemption of stored value in the SVFs		
1	Effective policies and procedures to ensure timely redemption of stored value.	
2	Efficient refunds and convenient access to refund facilities.	
3	Sufficient low risk assets to match total stored value collected.	
4	Sufficient liquidity to meet redemption patterns.	
Principle 2: Holders should ensure that their SVFs operate in a secure and reliable manner		
1 2	Sound business continuity management. Comprehensive outsourcing agreement and robust assessment of service provider.	
3	Robust risk evaluation framework with effective security procedures and controls.	
Principle 3: Holders should ensure that the rights and responsibilities of all stakeholders of the SVFs are fair and clearly defined		
1	Liability of each stakeholder in loss events.	
2	Protection agreements for stored value.	
3	Users' rights to obtain refunds.	
4	Fees and charges users and merchants have to incur.	
Principle 4: Holders should provide adequate disclosure of the users' rights and obligations		
1	Provide every new user with a copy of the agreement upon purchase.	
2	Update customers of any significant change in the T&Cs.	
3	Inform customers the holder is responsible for the stored value.	
Principle 5: Holders should implement adequate measures to prevent the use of SVFs for money laundering and terrorist financing		
1	Load limit per SVF should not exceed S$1,000.	
2	Bulk purchases of SVFs should not exceed S$20,000 per transaction.	
3	Stored value should not be transferable between unregistered SVFs.	
4	Effective measures to identify unusual or suspicious transactions.	

Monetary Authority of Singapore