EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB OPERATIONS MANAGERS GROUP

June 2007

SUMMARY OF THE RESULTS OF THE SWIFT CONTINGENCY ARRANGEMENTS QUESTIONNAIRE

1 Introduction

As agreed in the OMG meeting of 7 February 2007, this note summarizes the main results of the questionnaire on a local unavailability of SWIFT[1] that was sent to the members of the OMG (see annex). The objective is to get a better understanding of contingency arrangements in place at individual institutions, to share information accordingly, and to explore ways for improvements.

Ten replies from commercial banks were received, as well as four replies from central banks. In some cases the replies from commercial banks markedly differed from those given by central banks, which is mainly related to its role of TARGET operator.

Besides certain general issues, which are discussed in section 2, three scenarios of local SWIFT unavailability were considered in this survey:

- Unavailability of the telecommunication lines to connect to the SWIFT Network. This scenario is discussed in section 3.
- Unavailability of the SWIFT interface. This scenario is also discussed in section 3.
- Failure of the connection between back office applications and the SWIFT interface. This scenario is discussed separately in section 4.

Section 5 reflects on the OMG discussion of February and June 2007 and concludes with the closure of the topic.

2 General issues on local SWIFT unavailability

From the responses received it appears clear that the local SWIFT infrastructure has been set up in a very resilient way, with high availability clusters and several lines from different providers. Four commercial banks and three central banks never experienced any outages so far. In those cases where a SWIFT failure occurred, penalty fees and lost interest were frequent. Some institutions also experienced duplication of payment transfers and certain reputation damages.

[1] A global failure of the SWIFT network was excluded from this survey.

The maximum tolerable outage ranges from 15 minutes (two institutions) to 6 hours (one institution). The common denominator seems to be around 30 minutes to two hours, depending mainly on the time of day, thereby making it hard to precisely quantify the maximum tolerable outage.

Payments related/directed to CLS, Euroclear, Clearstream, EBA clearing, TARGET and/or other RTGS systems are the most critical transactions for the majority of commercial banks in case of a non-specified SWIFT failure. For central banks, critical transactions related to monetary policy operations conducted via TARGET.

The alternatives in place to deal with critical transactions in case of a SWIFT failure are quite diverse. Most commercial banks do not see any alternative to SWIFT, thereby relying on the availability of the SWIFT network, as well as the resilience and redundancy of the SWIFT infrastructure. One institution also relies on the BT Radianz network, a provider of secure messaging services.

Contingency procedures in place are often manual, such as transmission via fax (tested/signed fax procedures). Fax is only regarded suitable as a temporary solution for a limited number of transactions. Telex is only referred to by one commercial bank and by the central banks.

One of the problems identified by the manual processing is the risk that payment instructions are submitted both manually and automatically and subsequently processed twice e.g. once via the contingency processing and once after a recovery of the original system. Therefore, it is of utmost importance to be able to have a clear view on the transactions being queued as well as having the possibility to cancel transactions from the queues

3 Unavailability of the communication lines from the SWIFT interface to the SWIFT Network / Unavailability of the SWIFT interface

With respect to the resilience of communication lines and SWIFT interfaces, network components are at least duplicated by all with lines provided by different network partners. Dual-P connections[2] on different sites following different routes with automatic switching have in most cases been implemented. Duplicated SWIFT interfaces installed on different servers and cluster configurations for SWIFTAlliance Access and SWIFTAllianze Gateway[3] are the norm. Sometimes completely separated systems have been established at a third site.

Concerning the preferred contingency alternatives, some of the replies show satisfaction with the present infrastructure, given the lack of feasible alternatives. Some interest to implement a third site to connect to SWIFT has been shown as well. One institution encourages investigation of the possible usage of IP/internet based contingency solutions in order to process the most critical payments, while another

2 One of the connectivity packs that can be used to connect to the SWIFT Network., this package consists of an active/standby configuration with two VPN boxes, both of which are configured with a router and a permanent leased-line connection.

3 This is interface software provided by SWIFT enabling to connect to the SWIFT Network

institution expressed a preference for a secured mail solution. Others have pointed out that it would be preferable to have a unique fax procedure signed by authorized users with call-back confirmation without any telegraphic test keys.

4 Failure of the connection between Back Office applications and the SWIFT interface

The business continuity arrangements in place for the back office interface differ widely, depending on the number of transactions for the respective institution.

On the one hand, in case of a limited number of operations, manual procedures may be an option, but duplicated links between the back office application and the SWIFT interface software are usually necessary to lower operational risk. Although a standalone SWIFT interface may be a solution for manually entering transaction details, this solution is time-consuming, error prone and not suitable in case of a large amount of transactions.

Manual procedures are not suitable to process a high transaction volume. Only four commercial banks rely to a limited extent on manual procedures. Payments are prioritized in case not all payments can be processed, thereby postponing those payments with low value and low risk.

Commercial banks rely on clustered environments with full redundancy and multiple interfaces with automatic switching between back offices and the SWIFT infrastructure. Messages may be stored in queues and, once the connection is resumed, messages are re-routed automatically. Although a couple of commercial banks find a standalone SWIFT terminal suitable, the great majority is opposed to this solution, with the main reason being that this solution can be suitable only for a limited number of urgent and high value payments.

It was also reported that a standalone SWIFT terminal is not needed when the regular data entry functionality of SWIFTAlliance Access is used and that manual payments may sometimes be processed faster by the respective payments departments.

Secure internet browsers - so-called HTTPS interfaces - are used by one institution to manually input transaction details into SWIFT. In certain situations the SWIFT Alliance Webstation, SAB, can support the manual input of transactions for further processing over the SWIFT IP network.

5 OMG concluding remarks

Some general conclusions may be drawn:

Financial institutions have set up their local SWIFT infrastructure in a very resilient way, with high availability clusters and several lines from different providers;

In case of a SWIFT failure, each institution potentially incurs the risk of penalty fees, lost interest and duplication of payment orders as well as the obvious risk of increasing the potential for fraudulent payments.

- In addition to contingency solutions provided by the infrastructure providers e.g. CLS, TARGET, etc., manual procedures based on callback or tested/signed fax procedures are often referred to as an alternative in case of a total failure.
- Manual procedures are time-consuming, error prone and not suitable in case of large transactions.
- In order to avoid possible duplicate payments, measures should be in place i) to clarify the processing status e.g. which payments are processed and which are still in a queue as well as ii) to avoid duplicate processing once the infrastructure has recovered.
- The joint failure of SWIFT and contingency solutions may engender reputation damages.

In conclusion, the assessment and discussions revealed that OMG members were generally satisfied with existing bilateral arrangements. As such, it was commonly agreed to close this topic.

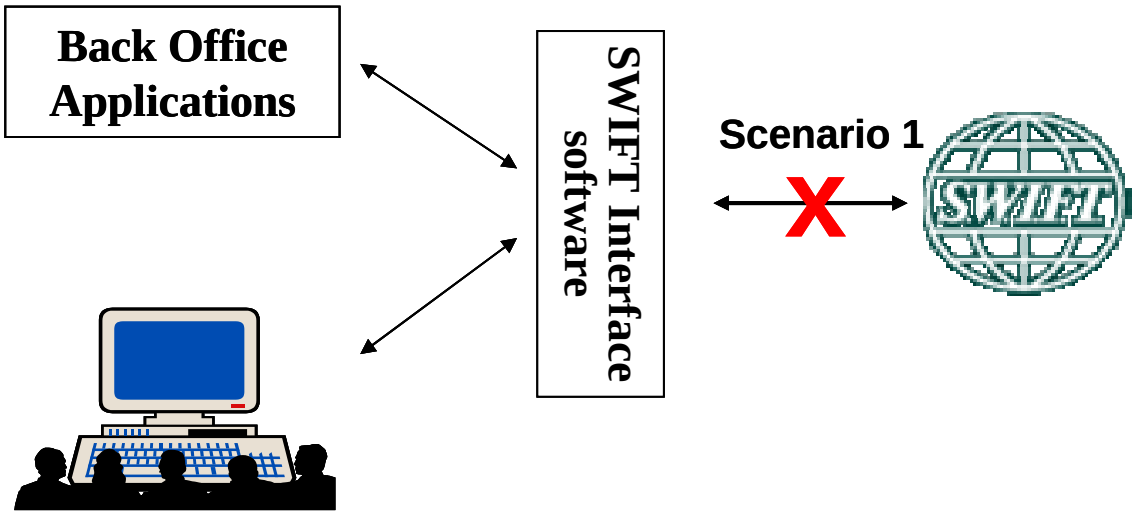
Annex 1 Questionnaire on a local SWIFT unavailability

The objective of this questionnaire is to get a better understanding of the contingency arrangements in place at the individual institutions in case of a local SWIFT unavailability. A global failure of the SWIFT network has been excluded in this questionnaire.

General

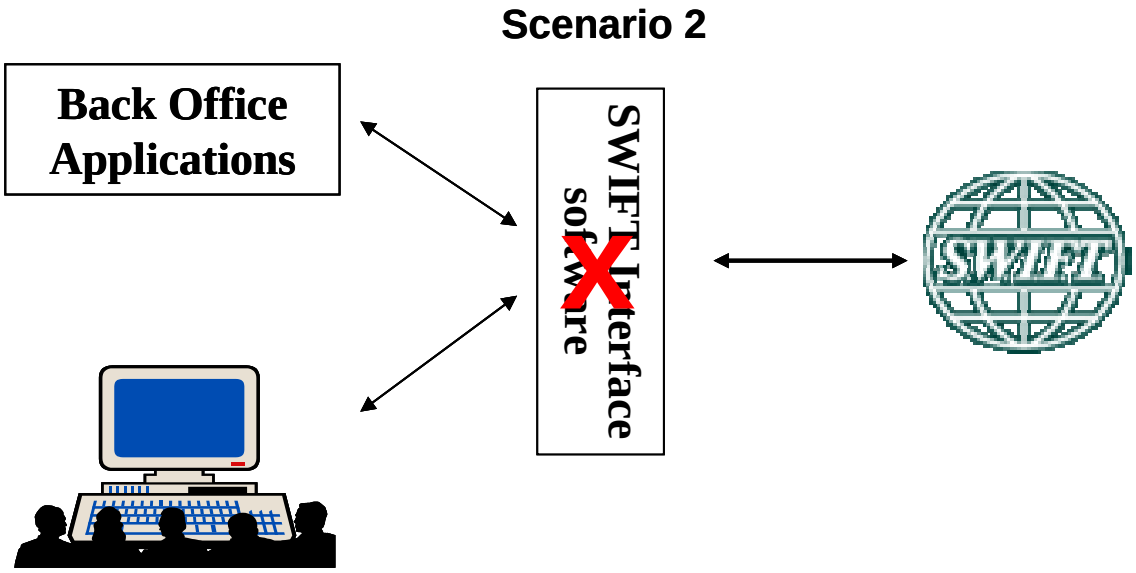
1. What is your maximum tolerable outage for a local SWIFT unavailability?
2. In case of a non-specified SWIFT failure, what type of transactions are the most critical transactions e.g. payment instructions to TARGET?
3. What kind of alternatives do you have in place for these critical transactions?
4. If the standard business continuity arrangements fail, what kind of contingency procedures do you have in place e.g. .tested telex? tested fax? internet solution ? others ??
5. Has such outage ever occurred to your institution? If yes, please describe:
    a. solutions / countermeasures adopted
    b. eventual manual actions with messages/payment instructions (check for duplications, matching, etc)
    c. consequences of the event for your institution (e.g. penalty fees, losses)

Scenario 1 – Unavailability of the telecom lines to connect to the SWIFT network



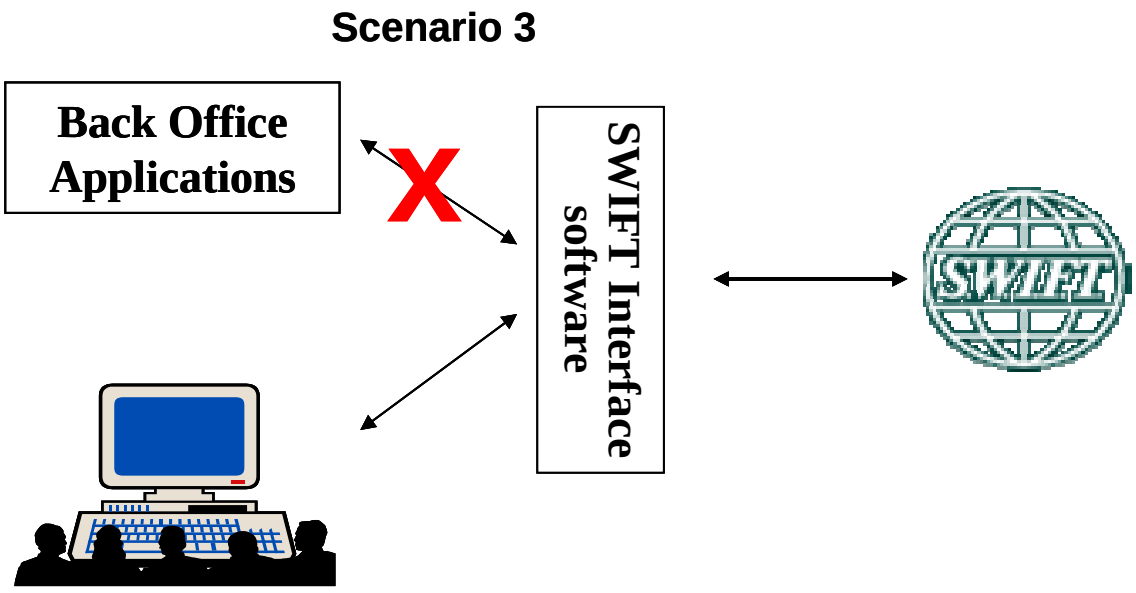
1. What kind of resilience do you have in place for these lines?
2. What kind of contingency alternatives would you prefer?

Scenario 2. – Unavailability of the SWIFT interface software/hardware connecting the back office application with the SWIFT network



1. What kind of resilience /business continuity arrangements do you have in place for the SWIFT interface?
2. What kind of contingency alternatives would you prefer?

Scenario 3. - The interface between the back office application and the SWIFT interface software/hardware



1. What kind of resilience /business continuity arrangements do you have in place for the back office interface?
2. Is a standalone SWIFT terminal/workstation a solution for manually entering the transaction details? others
3. What kind of contingency alternatives would you prefer?