GUIDE TO....

ATM MONITORING

Towards Intelligent Monitoring at
Windows-based ATMs

levelfour

GUIDE TO....

ATM MONITORING

Introduction

ATM networks have changed very little since their inception. IBM's withdrawal of support for OS/2 - the long-reigning favoured operating system for ATMs - at the turn of the 21st century, instigated a period of sustained change. According to Retail Banking Research, OS/2 usage is decreasing by around 8 to10 percent a year, and will be phased out over the next 4 to 5 years. Although global adoption rates vary according to analyst research – today, Retail Banking Research estimates 64 percent in Western Europe and Dove Consulting projects 63 percent by 2008 in the US – Windows has become the ATM operating system of choice.

Industry leaders recognise that Windows heralds the move away from proprietary to open standards. As hardware and software become 'decoupled', deployers are no longer locked into the proprietary software that accompanies an ATM terminal. This has changed the business models of ATM deployers as they have adopted a multi-vendor strategy to benefit from the more competitive pricing structure created by the Windows environment. However, a number of areas have been overlooked when considering this migration, notably how ATM terminals are remotely monitored and controlled in the new environment. The outcome is that banks and payments processors are experiencing greater downtime at their ATM networks in the Windows world.

The move from OS/2's stable ATM environment to the complexity of Windows with its regular security updates to the operating system, coupled with mismatched release cycles on the numerous other applications now resident on the ATM, impacts the ATM channel significantly. With new levels of risk introduced into the networks, ATM deployers need to monitor and control all elements more closely to ensure a profitable and reliable ATM network in the 21st century.

This guide has been designed to help ATM network deployers understand the business value of advanced ATM monitoring in a Windows environment. The Guide will outline the business and technical issues that banks and processors should consider when seeking to extract greater intelligence from their ATMs and put more intelligence back into the network.

Key pressures affecting the maintenance and control of ATM networks

With over 1.5 million terminals in service worldwide, financial institutions recognise that the ATM is a key customer touchpoint and have attached increased value to it beyond simple cash dispensing. Intensified economic and business forces have placed extraordinary pressure on banks to remain competitive, increase customer loyalty, and improve the efficiency and profitability of their ATM networks. These pressures are compounded by the fact that, given ageing legacy systems and rapid consolidation in recent years, banks now manage an increasingly complex mixture of vertically siloed technologies.

In order to get the most from their ATM channel, business owners must look to maximise the investment they have made in hardware and infrastructure as part of their migration to a Windows/open standards-based network and beyond. This has to be done alongside the ongoing challenge of addressing key pressures that affect the maintenance and control of ATM networks as well as minimising the ongoing cost of ownership of the network. Outlined below are some of the key pressures that business owners face that affect the maintenance and control of their ATM networks.

The time factor

Banks are under more pressure than ever to prove the profitability of the ATM network by extending their core ATM capabilities but are still struggling with other factors such as reducing the cost of ATM network maintenance and maximising availability. While ideally any fault at an ATM terminal should be raised as soon as it occurs in order to be promptly fixed, the reality is that there is often a significant time-lag from when a fault occurs to when the network operator is made aware of it or identifies it - in some cases, hours or even days.

The current approach largely relies on 'listening' to messages at the host and trying to interpret or 'second guess' what is happening at an ATM. For example, it may be several hours before a fraud detection platform senses that an ATM terminal has not performed transactions over an active period and then may raise an alert for an investigation at the ATM - Meanwhile the terminal has suffered a software fault unbeknown to the host, and customers have been unable to perform any transactions.

The data available to network deployers about the state of ATM machines lacks granularity so they do not know the specific nature of a fault at the ATM. This leads to longer delays in routing the problem to the correct department for investigation and resolution. The usual response is that ATM deployers send engineers to attend out-of-service ATMs without knowing the nature of the problem, which could be solved by a simple software restart. In the meantime, deployers suffer from the associated cost of network downtime, not only in terms of lost interchange revenues but also in failed customer interactions.

Customer satisfaction

ATM downtime creates brand risk with both customers and within the highly competitive banking industry as a whole. Customers have come to expect ATMs to be available 24/7 and to provide a high quality, stable service. In fact, widespread ATM downtime has achieved national newspaper coverage with the associated damage that causes to the bank's reputation. Low network availability and bad service can also be an embarrassing prospect for financial institutions when banking industry peers are presented with, for example, a monthly account of their country's ATM network statistics.

As such, quality is particularly important for deployers when introducing new functionality at the

ATM. However, it is difficult to evaluate how successful the uptake has been or what errors have occurred after deployment without closer monitoring of the network. Accurate monitoring post-release helps to gauge the success of each new software release. As banks embrace the value of customer loyalty and retention as opposed to the historic focus on winning new customers, it is essential that there is a consistently high quality of interaction across all banking channels.

A survey conducted by ICM research on behalf of Level Four in July 2007 indicated that 38% of respondents (UK cardholders) would consider moving their main bank account if their bank's ATMs were constantly out of service or unable to dispense cash.

Operational inefficiencies

An area of ATM operations that often causes overhead in time and cost is journaling - the process that gives the deployer a record of the exact sequence of events occurring at the ATM. However, for many, journaling is still largely paper-based, which involves a physical check on the journal roll inside the ATM to resolve any discrepancies. This approach results in lengthy delays in complaint handling that customers will not tolerate. Due to the high overhead of investigation, in some instances claims are not contested and revenue is lost. What is required is a centrally held journal database derived from device level logs, accessible from a customer contact centre to reduce operational cost and drive out inefficiency.

Dynamic inventory management

Another issue faced by ATM deployers is trying to understand the exact status of the different hardware devices and software versions across their ATM network, especially in view of the number of third parties constantly replacing parts through servicing ATMs, and also different service arrangements they may be managing in a multi-vendor environment. Deployers require a dynamic inventory database of all peripherals and software versions at individual ATM terminals that they can query at any time and receive real-time responses. The information would then be kept in a central repository where the deployer would have a dynamic and accurate picture of its ATM estate. This approach would enable it to route service calls with certainty (for example, to ensure the correct part to fix an 'out of order' ATM is sent the first time) and conduct software updates only on machines requiring updating.

Consider also the example of a bank looking to deploy ATM advertising, or other enhanced content on their terminals. This type of graphical/animated content requires the correct formatting in order to display correctly and so the deployer needs to have accurate data about each terminals specific capabilities, eg screen resolution and graphics cards in order to display properly. Many banks have lost track of the capabilities of the ATMs they own, making a project such as advertising extremely daunting without an agent-based monitoring approach.

Remote diagnosis of software faults

Software problems are the biggest causes of ATM failures. To prevent long periods of network downtime and the associated loss of revenue, ATM deployers need the ability to perform 'keyhole surgery' in order to stop and restart Windows processes at individual ATM machines.

Measurement and reporting of ATM uptime

In the OS/2 world, ATM availability was measured at the host and reported from the IT area within a bank to the business area. This was a valid approach for old communication protocols (like SNA) with a real point-to-point connection between the host and the ATM. Today, most banks use TCP/IP as a comminications protocol which does not use a dedicated host connection and so ATM availability is decoupled from network availability. As the majority of today's host systems are based on fault-tolerant computing and well established software, ATM network availability was high (often in excess of 99%). This is because the OS/2 operating system and application software were deemed very reliable, hence it was taken as a given that if the host was available for processing transactions, the ATM was available and in service.

However, in a Windows network, this approach is no longer valid because true ATM service availability can only be measured at the terminal. This requires constant reporting from the ATM terminal itself because transaction processing cannot happen by definition if an ATM terminal is not in use - even if the host is available. For a true and fair representation of ATM network availability, periodic 'heartbeat' reporting to a central server is

required to report on whether the ATM terminal is online and operational and able to accept customer transactions.

Greater visibility and transparency of the ATM network information to both IT and business departments will ensure and help to justify the closer alignment between them. They will also improve the quality and accessibility of true network statistics and information for management.

Security and risk management

Security is an issue high on the list of financial institutions' pressures. ATM networks are still subject to fraudulent attacks, even more so since the introduction of chip-enabled cards in much of the world that has forced fraud to migrate away from the Point of Sale (PoS). While there are a number of approaches to counter ATM fraud, closer monitoring of customer interactions at the ATM through video or photographic snapshots would provide ATM owners with a greater level of security.

Within the networks themselves, security is an issue. There is an emerging trend to grant third-party service agents access to a limited amount of diagnostic information about the network directly. While this offers obvious benefits, it also introduces a level of risk around network security that needs to be considered.

Loss of interchange revenue

Network downtime is a worst case scenario for deployers, especially for processors who manage multiple ATM networks, as it is costly in terms of lost revenue and customer loyalty. If a deployer experiences significant downtime in their ATM network, they lose revenue from interchange fees for several reasons. They cannot attract interchange revenue by offering ATM services to existing and prospective customers. Additionally, existing customers will seek alternative ATMs with the likely scenario being that they will go to a competitor's ATM, and deployers will be charged more expensive interchange fees. This scenario compounds the problem of network downtime as well as the negative impact downtime has on brand and reputation with customers.

Exploiting the potential for multi-vendor networks

Finally, with M&A activity and consolidation within the banking industry combined with the proliferation of open standards brought on by the move to Windows, ATM deployers face the challenge of capitalising on the potential of multi-vendor networks. Having hardware from multiple vendors within a network introduces a new level of risk. It also impacts deployers' operations as they have to reassess how to manage their ATM network, especially in terms of terminal monitoring and ATM servicing. Instead, ATM deployers need to drive costs down to reap the benefits of open standards and increased competition between vendors for the hardware business. Banks need to carefully consider their choice of ATM software, monitoring software and third-party service provision by viewing each as a separate business case, if they are to benefit most from this opportunity to avoid any vendor lock-in strategies re-emerging.

Summary

In conclusion, the combination of external and internal pressures requires banks to gain greater insight into, and better understanding of, what the ATM network is doing for their business. The intelligence gained provides competitive advantage for banks, improving their overall business by providing visibility to never-before-seen trends, patterns and statistics. With more detailed knowledge of their ATM network's performance, network traffic and quality of service, banks can improve the profitability of their networks and better address customer requirements and needs.

Towards intelligent ATM monitoring

In order to gain the significant business benefits available from the intelligence gathered from closer monitoring of the ATM network, there are several steps that financial institutions must follow. These can help leverage the financial institution's investment in the Windows operating system and modern ATM hardware by improving efficiency of the network, ensuring high quality of service and driving revenue.

Beyond these steps, there are other considerations that financial institutions need to bear in mind for intelligent ATM monitoring. These considerations are a direct result of the ongoing business pain points financial institutions experience.

What you need to do...

1. Ensure neutral monitoring

To date ATM monitoring has largely been conducted by 'listening' to the message traffic at the central host systems driving ATMs. This approach is limited in scope because it relies on interrogating the message traffic between the host and device and 'second guessing' the status of the ATM. The available data is stored in log files, not easily accessible and does not provide a holistic view of the ATM network. This is because ATM peripherals cannot be queried directly and there is no interface to the critical Windows operating system data. Another approach is that monitoring is sometimes provided by the ATM manufacturers as an additional maintenance function. This approach enables manufacturers to keep proprietary control of their hardware or software within the customer site, and, importantly, control the reporting process.

In the open standards world of multi-vendor ATM networks, prompted by the migration to the Windows operating system, financial institutions should ensure monitoring is independent of any ATM manufacturer. In order to achieve a true and accurate picture of how its ATM hardware, software and network is performing, banks should ask themselves whether they should entrust the critical monitoring function to a third party that has a vested interest to ensure that its hardware (or software) is seen to perform as well as possible in the bank's network.

Neutral, independent ATM monitoring opens up the possibility of being able to benchmark and compare hardware performance - such as overall machine reliability or to compare response times from different types of cash dispenser - to make better informed and cost effective hardware choices for their network. Using this data in an intelligent way will ensure optimum ATM network performance and operational efficiency over time.

A successful multi-vendor strategy in an ATM network therefore necessitates specialist agent-based independent monitoring and control software. Such software provides an unbiased and detailed view of the status of the hardware, software, and operating system on each terminal. Monitoring and control can be more efficiently provided via an independent monitoring and control server rather than the central financial host, allowing the central host to focus on providing efficient transaction processing.

To reap the true benefits of a multi-vendor strategy, ATM deployers should think about hardware, software and monitoring separately. Only then will ATM deployers gain unbiased

performance statistics across their network. To avoid vendor lock-in, ATM deployers must look at building and justifying a business case for ATM monitoring solutions in isolation of ATM software and hardware, being careful to question the motivations of those vendors touting 'bundled' deals that have been prevalent in the market to date. Independence is the key in running a profitable ATM network.

2. Define what is wanted from the network

Intelligent agent-based ATM monitoring enables financial institutions to view diagnostic and 'heartbeat' information from all ATM terminals within the network and therefore have more control over it. However, it is imperative to define exactly the metrics the business wants from the ATM network before embarking on an advanced ATM monitoring initiative. Another prerequisite is to determine how both the business and the IT/Operations departments of the ATM deployer want to report and analyze the data. A monitoring solution should provide the data in a customisable and granular form, easily accessible to all parties in real time. The size of the ATM network will be a significant factor in this.

The areas to define include:

- **What** to monitor. For example, if a new software release has been deployed within a particular group of ATMs, the Operations department monitors those ATMs more closely to ensure errors are dealt with quickly and efficiently to achieve and maintain a high quality of service in pilot or early rollout stages.

- **When** to be alerted to the status of the events in the network. For faults at an ATM terminal, the Operations team needs to be alerted as and when they happen to ensure a faster and smarter response as well as high network availability. Events such as approaching low disk space or low consumables may require a less time-critical approach.

- **How** to be alerted. Organisations create an event trigger and associate it with an alert to a specified user group or department via a range of communication channels, including email and SMS.

- **Who** receives the alerts. The business department chooses who receives the alert triggered by the event. For example, the alert of a physical fault at an ATM is sent directly to a management centre that dispatches a maintenance engineer to the specified ATM. However, a localised software fault may trigger a command for the internal operations centre to restart a process within that specified ATM terminal.

3. Empower business users

The centralised model for ATM monitoring traditionally favoured the IT department in terms of information flow. With ATM monitoring no longer controlled centrally and with greater transparency of network statistics, financial institutions can enforce an organisational change with the balance of power lying with the business users. They can grant different departments access to the information that is directly relevant to them, formatted appropriately, based on rules created and maintained by the business users. Accurate and timely business information reporting will enable business departments to better manage third party service agent SLA's, and have a better feel for where problems lie and resource allocation is warranted.

4. Become proactive

With the right intelligence in the right hands, business users can concentrate on new revenue generating and customer-focused service ideas and how to deploy them. The added intelligence from the network means that they can look at the network in new ways and become proactive rather than reactive An example is to monitor customer behaviour patterns after piloting a new transaction at a group of ATMs machines.

Financial institutions have the ability to increase revenues, not only by increasing interchange through increased uptime, but also by introducing new services at the ATM in a controlled way. By having reliable and accurate statistics of transaction patterns at the ATM, business users can tailor their offering to suit particular ATMs. For example, they could offer fast-cash menus earlier in the transaction at ATMs with the highest withdrawal volumes such as on a busy high street.

Other considerations

1. Change management

Change affects many aspects of the bank beyond the ATM network, including card issuing, customer support and internal operations. As the ATM is a direct channel to the customer, banks have to ensure that any change does not negatively affect the customer's experience at the ATM.

The recent EMV (Europay, MasterCard, Visa) smart card mandate in many parts of the world is a recent example of significant change that banks have to manage. With EMV, in the near future, banks need to be fully prepared to manage the addition of multi-applications onto their chip cards. Extending the ATM software to handle application downloads onto customers' cards, for example, would require close monitoring by the bank. The move towards deposit automation and cash recycling is also forcing changes for banks that need close management.

Change also affects the organisation itself. In other words, changes that impact network availability will also have knock-on implications such as staffing of helpdesk enquiries or internal operations processes.

2. Flexibility for the future

An independent, agent-based approach to monitoring provides the flexibility for banks to be prepared for the future in terms of adapting to change but it also addresses the immediate business pain-point of improving the profitability of the ATM network. It is imperative that banks choose a modern and flexible solution that is defined by what the bank wants out of its ATM network rather than a prescriptive solution from hardware vendors based on legacy technology. When all events are stored in a database on a central monitoring server, it will give the deployer insight into specific operational areas that previously would have been unattainable. Armed with better information, banks can make more informed choices in the future about hardware and software suppliers at a network level, and also make more granular choices, including what functionality to offer at particular ATMs.

3. Third party service contracts

The contracts banks hold with third parties such as service agents are often standard and do not take into account variations in the network such as locations of the most lucrative ATM sites. Given better insight into the profitability of an ATM network, banks should prioritise key sites and vary their contractual agreements with third parties accordingly. This approach should also include the priority attached to service calls to ensure that the ATM network is profitable and that key ATM sites have high levels of customer satisfaction. For example, a deployer would want its high priority site in a city centre location that failed on a Saturday evening to be fixed ahead of a device failure in an off premise supermarket location when the store is closed.

Furthermore, an agent-based approach enables ATM deployers to grant limited access to third party service companies, who can use this information to improve their overall quality of service to the bank. Sharing valuable information with partners enables them to minimise the number of service calls to the ATM, for example, by having accurate information about which replacement parts are required to fix an 'out of service' ATM.

4. Business Intelligence (BI)

Banks can use the data collected via intelligent ATM monitoring for competitive advantage by implementing best practice at an operational level and also in terms of making more informed business decisions for better results.

Improved business intelligence through advanced monitoring can be used throughout the bank's operations to:

- Improve overall network uptime
- Manage third party service relationships better
- Make informed purchasing decisions about ATM hardware and software
- Ensure transparency of reporting and strengthen Business/IT relationship
- Improve change management processes by utilising deeper knowledge of current systems, and ability to closely monitor rollout process

Technical considerations

Before advanced ATM monitoring becomes possible, financial institutions need to consider some technical points.

Agent-based monitoring at the ATM

An intelligent ATM monitoring solution has an agent on each ATM terminal that sends and receives data in real-time to a central monitoring server, independent of the existing financial host. This approach ensures that faults within the ATM network are dealt with quickly and gives the banks a holistic view of the network with much improved granularity. Conversely, traditional ATM monitoring from the host does not have the capability to look at each ATM terminal in real-time. The latter relies on transaction message traffic to "guess" what is happening at the ATM rather than proactively investigate. A sophisticated agent, however, would have access to the (XFS) layer to query devices and the ability to access operating system data through the Windows Management Interface (WMI). An agent-based monitoring approach ensures that any problem at the ATM terminal is identified and dealt with immediately, resulting in lower ATM network downtime. It also means that central host systems can focus on their core functionality of transaction processing.

Web-based access to monitoring information

The dissemination of the information gathered from ATM monitoring needs to be easily accessed by recipients. A web-based model ensures that users across the organisation can access the information directly from their intranet browser on their desktop and tailor how they would like the information presented – a personalised ATM network dashboard – whether for an operational, business or technical audience.

Network size

As every ATM is monitored within the network and information is constantly being reported from each machine, financial institutions need to consider available network bandwidth and the size of the monitoring server in relation to the size of the ATM network. The right server configuration is particularly important in financial institutions with larger networks because appropriate failover capacity needs to be in place to ensure uptime is preserved. Server and database configurations should be based on industry standard open technology for scaling the business up easily.

Security

The move to Windows at the ATM has opened up the network such that banks have many more back-end connections to various service providers and internal subsystems. Banks need to define and police new processes so that they know who has ownership in particular situations. They also need to determine who has access to information at different connection points to ensure that the network is fully protected, and every participant is aware of others in the chain.

Importantly, an intelligent ATM monitoring solution needs to sit alongside the ATM's security platform, with roles and responsibilities clearly defined and understood.

The XFS open standard

The XFS open standard plays an integral role in an open environment because it provides a standard way for an application to communicate with all peripherals. If a bank is using a non-XFS monitoring solution (or only partial XFS with some manufacturer specific additions) by definition this is a proprietary approach designed by an ATM manufacturer to monitor their own hardware/software. Banks looking to exploit an effective multi-vendor strategy in their ATM networks should keep XFS firmly in mind when making hardware, software and monitoring solution choices, and insist on true compliance from all vendors.

Independent testing

Before the introduction of new services at the ATM, it is imperative that they have undergone a comprehensive testing programme. Just as monitoring needs to be independent, the testing process should also be viewed in isolation to ensure that all possible errors have been identified and corrected prior to deployment. Thorough testing will ensure a reduction in preventable software faults before they are released into the network – a common problem affecting ATMs today.

An automated testing regime for Windows-based ATM applications and end-to-end network connections is accepted as best practice within the industry.

Future opportunities at the ATM

The migration away from proprietary technologies and the OS/2 operating platform has been a big step forward for banks and payment processors. The complexity of the migration is further compounded by the requirement for a new version of the application software that runs under Windows. In many parts of the world, this has involved banks moving to a Windows version of their existing ATM application software (for example, NCR's APTRA Advance NDC and Wincor-Nixdorf's ProCash NDC) that are essentially new versions of old software. On the whole, these have been built around the XFS open standard but still use the same host messaging protocol as before. The upgrade in operating systems often goes hand in hand with a network migration to TCP/IP. In order to support the system requirements of Windows (and industry mandates such as EMV for some countries), in many cases a wholesale upgrade to the ATM hardware estate is also required.

After banks invested in a new Windows infrastructure, many started to question the business case of the migration. For most it has meant a modest improvement in the branding capabilities at the ATM but it has introduced massive overheads in terms of testing, and overall reliability of the networks has decreased. This is largely due to the increased number of 'moving parts' in the ATM software stack, the frequency of change of ATM software updates and operating system security patches. Many industry observers would argue that this migration and decreased reliability has brought effective ATM monitoring into the spotlight as a key factor in ensuring a reliable ATM network in the Windows era.

As the ATM channel moves away from a world of proprietary, legacy applications towards embracing open standards, a number of significant changes are occurring that open up the opportunities at the ATM:

- XFS matures: As the XFS open standard continues to mature, ATM manufacturers' margins are being cut with regards to ATM hardware as the hardware market becomes more and more commoditised.

- Software is key: Software is becoming the key to unlocking value from the ATM channel and delivering the business case for wholesale upgrades to the ATM network and the Windows operating system.

- Change in software architectures: The existing software architectures (whether dumb terminal legacy applications or bespoke fat client applications) are outdated now that many banks have upgraded to high-bandwidth TCP/IP connectivity. Emerging, distributed software architectures that allow secure connections to third party systems (for example, CRM, advertising servers or third party content) are becoming the accepted industry direction for ATM software. The architecture is through standard web services interfaces that are not reliant on the existing financial host.

- Holistic software lifecycle: Banks should think about the software lifecycle as a holistic combined process - including areas such as effective monitoring and automated testing – rather than only application software. This approach is becoming more important for running a successful ATM network

Conclusion

The migration to Windows and the associated opportunities it provides will be to the advantage of most banks and processors. However, ATM deployers need to make a strategic decision regarding their ATM monitoring. Historically it has been embedded in the service and maintenance package of ATM manufacturers and been centred around the limited data available from the host system. But in a multi-vendor Windows environment, financial institutions need an independent monitoring solution at the ATM terminals themselves to provide greater insight into the performance status of their ATM networks, with data provided in real-time to business, operations, and technical departments.

To remain competitive in the ever-changing retail banking industry, the time to invest in advanced ATM monitoring is now due to the continued pressures to deliver sophisticated, revenue-generating customer services and to maximise network uptime. Deployers should keep in mind the significant benefits that employing an independent strategy for ATM monitoring can bring, and use this to their advantage when making ongoing decisions about ATM hardware and software.

European sales and support

Level Four House
Pitreavie Court
Pitreavie Business Park
Dunfermline
KY11 8UU
UK

Tel: +44 (0)1383 720118
Fax: +44 (0)1383 720119

Middle East sales and support

Al Thuraya Tower 1
2nd Floor, office 209
Dubai Internet City
P.O. Box 500274
Dubai
UAE

Tel: +971 4 368 1808
Fax: +971 4 368 8091

Level Four Americas

Level Four Americas LLC
5960 Fairview Road
Suite 400
Charlotte
NC 28210
USA

Tel: +1 (704) 837 8050
Fax: +1 (866) 560 9783

enquiries@levelfour.com
www.levelfour.com

levelfour