MICRO SOFTWARE DESIGNS

MSD Newsletter

Volume 3, Issue 2
December 30, 2007

SEASONS GREETINGS !!!

We at MSD would like to wish all of our valued customers an enjoyable and safe Christmas season and New Year. As 2007 comes to a close, we want to thank you for your continued support and we look forward to continued fruitful partnerships in 2008.

MERRY CHRISTMAS & HAPPY NEW YEAR

from ALL OF US !!!!

In this issue:

LET'S TALK ABOUT I.T.™

Belize

Our customers in the lovely country of Belize were exposed to a wide array of MSD products alongside the technical details necessary to inform the ATM connectivity process, via the inaugural session of our Let's Talk about IT™ initiative held at the St. John's Credit Union conference centre on Saturday 9th December 2007.

The primary objective of this session was to highlight the pros and cons associated with ATM connectivity. Participants were presented with different connectivity scenarios, with emphasis being placed on reliability, security, efficiency, cost and benefits.

Participants also benefited from being exposed to the intricacies of our Self Service Technologies (SST), namely, Global Information Access (GIA), Interactive Voice Response (IVR) and ATM On-line.

Our Shared Services product was also highlighted at this forum. Everyone present agreed that this product embraces the philosophy of the credit union movement, and once effectively implemented, has the potential to harness the co-operative spirit amongst credit unions, locally, regionally and internationally.

The level of readiness to adopt these technologies amongst institutions judged on a continuum is moderate to high.

St. Lucia

The primary objective of the St. Lucia Let's Talk About IT™ forum was to ensure all participants understood the intricacies involved in adopting the Shared Services product. Emphasis was placed on the fundamentals associated with the readiness to adopt this technology. Participants were also exposed to details associated with the effective implementation of this product.

Both forums were attended by Board members, managers, IT personnel and operational staff.

BREAKING NEWS !!!

MSD has launched an initiative to provide an Electronic Funds Transfer (EFT) facility to be implemented in the 3rd quarter of 2008. Discussions and system design have already commenced with the preferred Bank, who will provide the gateway to Linx, Visa and/or Master card. The products to be offered on a phased basis are:

- Linx Debit Card
- ATM on Linx Network
- International Debit Cards
- International Credit Cards

Features:

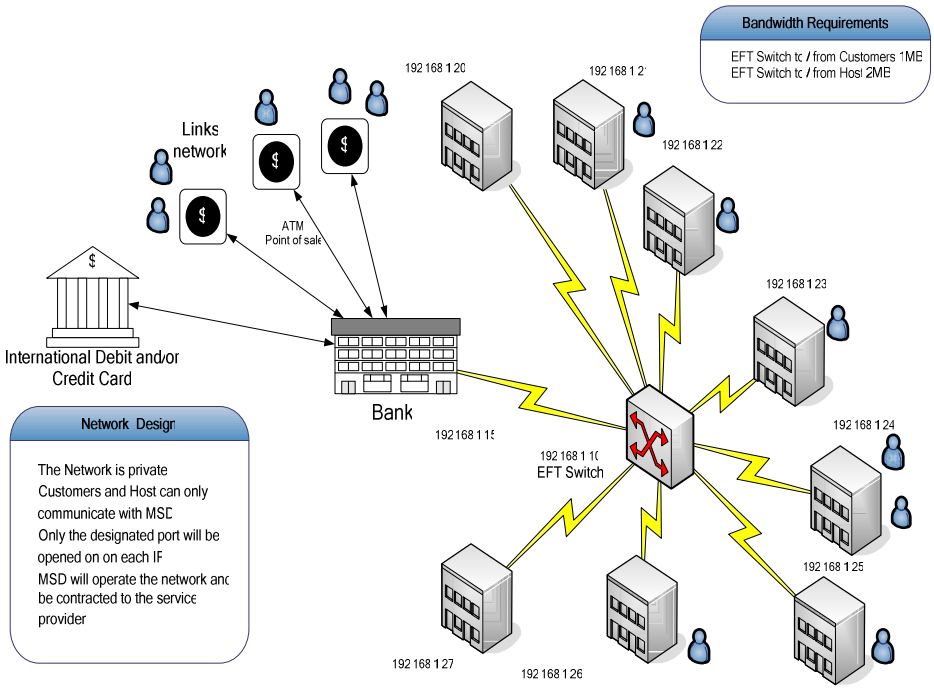
⇒ On-line, no batch processing

⇒ Automated, no manual entries

⇒ Real-time, no loop holes

We will be partnering with a USA based EFT Switch provider with whom we share mutual customers and a long and beneficial relationship. Our EFT Switch partner is also the provider of one of the region's foremost banks and provides EFT switching service throughout the region.

Proposed Dedicated Network



The communication network design has already been discussed with the preferred provider, Flow, using a high speed, dedicated, private network connection on a fiber optic backbone.

The system design allows for institutions to electively add ATMs to the Linx network. The concept is for the customers (who so desire) to purchase ATMs and install at locations of their choice. The customer can elect to make the ATMs available for use by their members only, or connect them to the Linx Network, thereby allowing any Linx-enabled card holder to utilize the devices. This business decision that will be decided by the ATM owners, in addition, the option to attach the ATMs to the Linx network must be sanctioned by Linx administrators.

In the first quarter of 2008, MSD will contact our customers to conduct a needs assessment, with a view to finalizing system design. Interested customers and other stakeholders can indicate the level of participation in the proposed venture.

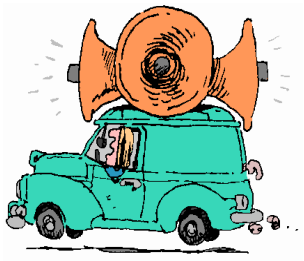
This venture is consistent with the government of Trinidad and Tobago's stated 20/20 vision and is a golden opportunity for non-bank financial institutions to embrace this facility, which will aid in fast tracking the non-bank, financial sector into a leadership position in ICT.

UPDATE ON CUMIS TC

We're pleased to report that the CUMIS Plus Thin Client (CUMIS TC) project is on schedule for release in the 2nd quarter of 2008. In order to ensure an on-time release, we will be implementing a code freeze commencing January 1st through April 30th 2008. The code freeze means that only modifications essential to business operations will be undertaken during this period. All non-essential requests for modifications will be deferred and implemented in the following release. Some of the new features that will be included in CUMIS TC are:

- Custom Report Composer
- Data integration with Microsoft Office products
- Ability to launch multiple modules simultaneously (Multiple Document Interface)
- Graphic User Interface for Linux Based customers
- No TunEmul Licensees
- Improved Performance

The new version, CUMIS TC will be available for demonstration via the Internet by March 31st 2008. Stay tuned for further developments.



UPCOMING EVENTS

Let's Talk About IT sessions

Jamaica : March 2008

Trinidad & Tobago: April 2008

Session dates are yet to be confirmed.

Site Visits

Jamaica—tentatively scheduled for January 2008.

Products on the Horizon

- Online Bill Payments
- Online Cell Top-up
- SMS-Direct
- GIA Central

FEATURE STORY - NETWORK SECURITY

Is Your Network Truly Secure?

IT managers are well aware of the threats to their networks, and have spent heavily on solutions to protect the corporate environment, but despite this expense, many organizations are not truly in control of their users.

In the drive for more flexible working, networks are opened to third parties, such as contractors, whose security applications are not subject to control by the organization. Additionally, administration rights usually granted to direct employees often compromises security by allowing critical security services to be disabled.

With no enforcement mechanism in place to drive compliance or report on results, the network is open to the hostilities of a threatening landscape that involves stealthy, targeted and financially motivated attacks to exploit these vulnerabilities in endpoint devices. Many of these sophisticated threats can evade traditional security solutions, leaving organizations vulnerable to data theft and manipulation, disruption of business-critical services, damage to corporate brand and reputation, and non-compliance with regulatory requirements. The complexity of managing modern security applications, combined with the lack of control of endpoint computers attaching to the network, has persuaded many security vendors to incorporate compliance and enforcement capabilities as extensions to existing products. For IT managers to maximize their return on investment, they need vendor-neutral solutions that work with their existing infrastructures, enabling them to take control of threats from malware and unknown or non-compliant users. The critical factor for successful implementation is an ability to define firstly, policies that can be applied to groups of users, and secondly, the membership of those groups of users appropriate to the organization's operations.

Technology and initiatives

Security experts agree that there is absolutely no way to eliminate every threat. What an organization can realistically do, however, is to assess and eliminate vulnerabilities, and have systems in place that consistently manage network security by looking for potential threats and adequately protecting enterprise resources. Therefore, access to the protected, managed, and already compliant network must be controlled by determining a connecting computer's level of security before allowing it to connect – and preventing access by non-compliant computers – and continuing to assess compliance once connected.

Network Access Control

Network access control (NAC) technology is a viable answer to solving the issues of compliance of all computers attempting to connect to the network, whether LAN-based or remote, managed or unmanaged. True NAC reports on the security status of a computer to be assessed against a predefined policy before it connects and periodically during a session, as well as enforcing policies that manage access at various levels, and provides for the remediation of non-compliant computers.

Network access control solutions should a) assess the security state of endpoint devices, b) compare against relevant policy, c) enable levels of access for remediation, d) monitor connections, e) enforce requirements and d) report.

Scanning determines the state of a computer's configuration, such as its application levels and security status. The information is sent to a policy manager that determines what level of network access is allowed, which is then implemented by the network. After the initial scan, and potential blocking, the network access control process directs non-compliant computers to remediation resources, monitors changes in the security state and network activity of connected computers, and quarantines any infected computers to minimize the threat to the network. Overall, NAC is capable of maintaining the network's original security state through proper configuration management.

NAC solutions can be standalone or they can be incorporated into the internal network infrastructure. The solution appropriate for an organization is primarily dependent on its current network environment, such as how homogeneous the network currently is, what the main network access methods are, and the budget available.

Phasing implementation

Administrators can implement a solution in a way that supports the progressive enforcement of security policy, as shown below.

- Create a policy that reports on the state of applications installed on endpoint computers;
- Update the policy to issue warnings for required applications that are not installed or running correctly, and provide links for users to update them;
- Update the policy again to provide enforcement and require remediation for non-compliant computers before they gain access to the network.

This flexible, phased approach is a much more workable alternative to an all-or-nothing deployment of security compliance, minimizing frustration for both users and hard-pressed IT departments.

Reporting

Effective reporting is essential not only in aiding the troubleshooting and analysis phases of implementing and managing security applications, but also in meeting regulatory compliance. Administrators need ready access to data in order to a) determine applications in use, b) assess applications against policy, c) track trends in compliance, d) update policies, e) distribute policies, and f) track changes to configuration and enable rollback.

Armed with this information, administrators are better able to change their enforcement strategies in relation to actual activity, depending on the threat level or simply if tougher enforcement rules are needed. In highly regulated businesses, the role of reporting is critical. Assessing and enforcing policies shows auditors that enterprise controls are in place and reasonable protection can be proven.

Conclusion

Organizations should not wait to begin addressing the issues of security compliance. Having a policy-driven security program in place to prevent unwanted network access and to protect the integrity of the network is essential, and can be achieved progressively, with minimum upset to users, without compromising existing network infrastructure. For further information, please contact the MSD Technical team at tech@msd-tt.com.

MICRO SOFTWARE DESIGNS

Corner Austin Street & Eastern Main Road,
St. Joseph,
Trinidad & Tobago

Phone: (868)663-2768, 663-3880, 645-6084
Fax: (868) 645-6084
E-mail: info@msd-tt..com
Web: www..msd-tt.com

"Committed to Software Excellence and Integrity"

NEED SUPPORT ?

"Sizzling...smoking...flames shooting from the hard drive.
OK...that IS a malfunction and you'd best unplug it."

Our dedicated and hardworking support team are standing by to assist you with your queries.

Vashti Paul-Khan	Senior Business Analyst	vashti@msd-tt.com
Marcia Moses	Technical Support Supervisor	marcia@msd-tt.com

Technical Support:

Patrice	Bobb- Semple	patrice@msd-tt.com
Gail	Griffith	gail@msd-tt.com
Shawn	Louison	shawnl@msd-tt.com
Shawn	Mills	shawn@msd-tt.com
Warren	Alexis	warren@msd-tt.com
De-wayne Berkeley		dewayne@msd-tt.com

COMMENTS ?

Your feedback is always welcome. Please send any comments about this newsletter to newsletter@msd-tt..com.

EMPLOYEE FOCUS

This year has seen quite a few changes in the organizational structure of the company.

Quality Assurance/Documentation

- Yvette Bobb has joined the team from the Technical Support team.
- Nicole Hernandez has joined the Quality Assurance team from the Adminstration team.
- Kiyomi Rankine has replaced Gail Mc Carthy as the Quality Assurance/ Documentation supervisor.

Technical Support

- Marcia Moses has joined the Technical Support team from Quality Assurance as the supervisor of Technical Support.

Administration

- Darcelle Goolcharan is our new Administrative Assistant (Operations).

Farewell and best wishes to Gail McCarthy and Rasheed Ali who left us to pursue other careers.

ABOUT US

Established in 1984, with over 130 clients throughout the Caribbean, MSD is the market leader in the development and support of multi-platform Management Information Systems software for financial and retail institutions.

We provide high performance, customized software solutions, and extensive support and training for our clients thus enabling us to achieve awards of excellence year after year.

We offer the following services:

- Software Development,
- LAN and WAN,
- Computer Hardware Sales,
- Consultancy.

Some of our software product front-runners are:

- CUMIS Plus (Credit Union Management Information Systems),
- iBOS (Integrated Banking On-Line System),
- WinPrint (Unix to Windows report previewing and formatting utility),
- ATM Simulator.

For further information, please contact us at info@msd-tt.com.

CONDOLENCES

We would like to extend our sincerest condolences to the family, friends and colleagues of Petronella Ettienne from COPOS Credit Union in Trinidad & Tobago on her recent passing. May her soul rest in peace.