

Would you like to centralize the control
of security of your ATM network?

YES



Wachovia Corporation

An NCR Case Study



Experience a new world of interaction

The customer

Wachovia is a diversified financial services company that provides a broad range of retail banking and brokerage, asset and wealth management, and corporate and investment banking products and services. It is one of the largest providers of financial services in the United States, with retail and commercial banking operations in 21 states from Connecticut to Florida and west to Texas and California, and nationwide retail brokerage, mortgage lending and auto finance businesses.

Wachovia Corporation has a large and growing automated teller machine (ATM) network as part of its highly successful financial services business. That network now includes 5,100 ATMs in 19 states plus Washington, D.C. The ATM network continues to expand through merger and internal growth.

Wachovia, like other banks, has requirements for ATMs that differ from its requirements for desktop PCs. ATMs are unattended, customer-facing devices that operate 24x7, that must maintain the highest possible levels of security and availability.

Key Highlights

- **Industry/Market:**
Financial/banking
- **Challenge:**
Wachovia wanted a way to centrally manage the security of its ATMs, in order to drive down the time and cost of ATM management.
- **Solution:**
NCR and Microsoft helped Wachovia give its Windows-based ATM network the levels of centralized security and manageability that the bank sought.

The challenge

Starting in 2003, the bank introduced a small number of Windows® XP Professional-based ATMs, running NCR's multi-vendor APTRA™ software, into its network. They were standalone units tightly locked down locally with APTRA security, policies and firewalls. Because remote access wasn't an option, a technician was dispatched to troubleshoot or reinstall the software onto an ATM whenever problems were reported. This was an expensive and time-consuming process. Wachovia wanted a way to centrally manage the security of these ATMs, in order to drive down the time and cost of ATM management.

The bank was implementing the Active Directory® service in Windows Server® 2003 across its corporate network but lacked expertise in the use of Active Directory for ATM networks.

One of the key challenges that Wachovia faced was to define the relationship between its ATM network and the rest of its enterprise infrastructure—which was already based on Active Directory.

• Results:

"Active Directory has given us the peace of mind that our security settings are being applied the way we want—in a consistent and timely way across our ATM population," says Greg Curry, Manager of ATMs, Information Technology, Wachovia.

"We chose Active Directory to enhance the manageability of our ATM security," says Brian Anderson, Senior Programmer and Manager, APTRA ATMs, Wachovia. "But once we started using it, we could see that it would yield manageability benefits far beyond security."

With the Active Directory implementation, Curry's staff can access the ATMs remotely—even without disturbing customer sessions in progress. Because Wachovia may avoid sending a technician to visit a failed ATM, it can save almost three hours per visit, avoiding the expense of site visits, and boosting ATM availability.

The solution

Wachovia turned to Microsoft and NCR—one of its primary ATM providers—for an answer. They proceeded to help Wachovia give its Windows-based ATM network the levels of centralized security and manageability that the bank sought. As a result, Active Directory, along with Windows XP Professional and APTRA multi-vendor software, became the foundation for a single ATM image, replacing the mix of software applications that Wachovia had used.

Centralizing the control of security, configuration and maintenance

The use of Active Directory allowed Wachovia to take advantage of centrally managed Group Policy settings, a powerful mechanism for distributing consistent security and configuration changes to large numbers of Windows-based clients.

Group Policy settings enable Wachovia IT technicians to update the security configurations of an entire ATM population without visiting the sites. And with Group Policy, Wachovia gains a reporting capability so that IT administrators can examine and review all of its configurations from a central point.

NCR and Microsoft delivered in-depth guidance and best practices on the use of Active Directory in the ATM environment. The two companies communicated their joint guidance to Wachovia through documentation as well as workshops with Wachovia staff.



Balancing competing needs

Best-practice guidance from Microsoft and NCR recommended that the ATMs be included in the Active Directory infrastructure—but isolated from the rest of that infrastructure. The guidance also suggested that the Windows XP Firewall be deployed to block unwanted traffic into the ATM network.

NCR contributed its self-service security expertise by advising Wachovia on how best to harden the domain controllers on which the Active Directory environment depended. And it provided the domain join script, which includes the removal of locally enforced policies and roll-back functionality, to help ensure the ATM would recover from any potential errors during the conversion process without requiring the manual reloading of software.

From design through to deployment

Microsoft and NCR evaluated and confirmed the Active Directory-based design that Wachovia's IT team devised, and the two technology companies assisted with all phases of testing and deployment. That testing included a month-long session at NCR's global research and testing facility in Dundee, Scotland, during which NCR and Microsoft engineers reviewed the proposed configurations with their Wachovia counterparts and probed the effects of changes in resource utilization, domain controller structures, and other variables.

The proposed architecture then went through four months of testing at Wachovia, followed by a series of pilots. The Active Directory-based design was first rolled out to ATMs at Wachovia's Charlotte, North Carolina, headquarters, giving the company's technical professionals a microcosm of an end-to-end deployment to evaluate. The deployment has continued in a series of increasingly broad rollouts.

"The combination of Active Directory and APTRA is definitely enhancing security as well as our ability to provide customer service and the quality of the customer experience we can deliver."

*- Brian Anderson, Senior Programmer and Manager,
APTRA ATMs, Wachovia*

Why NCR?

With over 125 years of experience and knowledge, NCR is a leading global provider of payments, assisted- and self-service solutions. NCR has been the global number one manufacturer of ATMs for more than 22 consecutive years. We help our clients around the world improve their customer interactions, implement change quickly and proactively, and transform their businesses to become leaders and change agents. We can help you, too.



NCR Corporation

2651 Satellite Boulevard
Duluth, Georgia 30096
USA

www.ncr.com



Experience a new world of interaction

NCR continually improves products as new technologies and components become available. NCR, therefore, reserves the right to change specifications without prior notice.

All features, functions and operations described herein may not be marketed by NCR in all parts of the world. Consult your NCR representative or NCR office for the latest information.

NCR APTRA is a registered trademark or trademark of NCR Corporation in the United States and/or other countries. All brand and product names appearing in this document are trademarks, registered trademarks or service marks of their respective holders.

© 2009 NCR Corporation Patents Pending EB10183-0809