



Global Bank Takes Proactive Steps to Secure and Expand Online Services

SUCCESS STORY

Challenge

- Protect customers from internet attacks
- Reduce operational costs
- Automate & improve customer service
- Support expansion of online services
- Comply with FFIEC requirements

Solution

Arcot alone offered a tested and proven single-vendor solution.

Result

The Arcot solution easily scales in size and functionality to support the desired range of future services.

This case study involves one of the largest global banking institutions in the U.S.

Challenge

This large financial institution wanted to satisfy FFIEC requirements and implement a strong two-factor authentication framework to provide greater identity fraud protection, minimize exposure of confidential information, and support future digital signing and e-statement delivery applications.

Solution

A comprehensive single-vendor solution from Arcot Systems provides a multi-layered security framework that encompasses strong authentication, risk management, encryption and digital signing. Arcot Professional Services' expertise facilitates a smooth and successful implementation.

Protecting Online Banking

With the growing popularity of online banking, this banking institution wanted stronger security safeguards for their Internet-based business. At that time, the bank already had more than 12 million online customers and was adding about half a million new users each month. Given the threat posed by sophisticated electronic attacks, the bank's IT organization was determined to minimize the risk of fraud and the potential for exposure of confidential information.

With plans to move even more critical business processes online, the bank's IT group knew that their existing infrastructure alone would not be adequate to support and secure the advanced applications they would launch in the future. Although this was prior to the onset of government regulations (FFIEC in the US and HKMA and MAS in Asia), they wanted to implement strong multi-factor authentication in order to protect their online business systems. In doing so, however, it was critical to minimize change to the user experience.

Looking beyond the immediate security issue, the IT organization also wanted to leverage a scalable framework in order to support the kinds of advanced capabilities that would continue to improve their return on investment (ROI). By

expanding their portfolio of online services, the bank would reduce operating costs while increasing their competitive edge. They were interested in converting to encrypted statements (e-statements) and replacing traditional "print and sign" approval processes with digital signatures. This would not only make applications for new services faster and more convenient for customers, but would also verify both the authenticity of a signer's identity and the integrity of a document's contents.

Searching for Excellence

The bank was seeking a scalable long-term authentication solution that would carry them well beyond their initial basic deployment. They wanted a comprehensive yet easy-to-use framework with built-in support for additional services and various levels of authentication, up to and including digital signing. They needed a robust solution with the ability to withstand man-in-the-middle attacks. And, it had to integrate with the CA SiteMinder Web access-management product, which would be easier to achieve with a software-based solution.

The bank's future plans included using digital signing of electronic documents to minimize the time lag associated with the printing, signing and transmission of traditional paper documents. This would enable the processing of loan and account applications more rapidly and cost effectively, while at the same time improving customer service. Use of non-repudiation capabilities and audit trails would make even high-risk transactions viable candidates for online conversion

Unlike some competitive banks that were deploying short-term fixes, the IT group opted for a well planned, thoughtfully designed and carefully implemented system that would incorporate strong authentication and digital ID protection. In short, they insisted on nothing less than a "do-it-right-the-first-time" deployment.

The organization initially looked at 38 vendors and then narrowed the list to about seven that warranted an in-depth assessment.

The bank's key decision makers felt confident, knowing that Arcot understood identity and access management issues and would be able to guide and assist them in these critical areas.

A Proven Solution

All other competitive solutions involved integrating multiple vendors' products (with associated interoperability issues) in order to deliver the full functionality that the bank would ultimately require. In contrast, Arcot alone offered a tested and proven single-vendor solution. Plus, the Arcot solution was software-based, which would make it much easier to integrate with CA SiteMinder and the bank's existing IT infrastructure.

The bank's IT group chose the multi-layered Arcot solution because it combined strong authentication, risk management, digital signing and encryption with ease of use and scalability, thus addressing all of their requirements. Through a phased deployment that would initially require no change whatsoever to the online user experience, the Arcot solution would easily expand in size and functionality to support the desired range of future services.

Risk Management

To avoid any perceptible change to the online user experience, the bank initially limited activities to Arcot's risk management solution, RiskFort. This simplified the initial implementation and would continue to require only username and password during login. This ensured that the initial implementation would be, in the words of one of the bank's key IT staff members, "a non-event to the end-user."

Government regulations, such as FFIEC in the US and HKMA and MAS in Asia, require multi-factor authentication. The Arcot solution has already put the bank in full compliance with these industry mandates, even before their effective dates of enforcement.

Strong Authentication

From the beginning the bank was looking beyond merely complying with the FFIEC mandate. Risk management reduces the risk of fraudulent access but to protect the bank's online customers from more sinister attacks like Man-in-the-Middle, the bank plans to implement Arcot's true, two-factor authentication solution in the future.

Partnering with the Bank

To ensure a smooth transition, the bank relied on the Arcot Professional Services organization to direct and oversee the deployment. This assured the bank of having on-hand the necessary expertise to identify and fix any issues that might crop up during implementation.

The Professional Services team of Arcot experts managed installation of the multi-factor authentication solution and configured it to meet the bank's specific needs. The bank's key decision makers felt confident, knowing that Arcot understood identity- and access-management issues and would be able to guide and assist them in these critical areas.

In addition to overseeing the implementation, the Arcot Professional Services team also delivered an unexpected secondary benefit. They helped the bank improve the throughput of their online system by tuning their applications to run more efficiently. This partnership approach resulted in developing a better way for the bank to operate the Internet side of their business.

Planning for the Future

Ultimately, the bank will use the ArcotID software smart card for e-statements and digital signing which will dramatically reduce postage and cut the cost of existing business processes. Replacing cumbersome "print and sign" processes with simple-to-use "paperless" document signing streamlines business approval processes. This will automate online applications for new banking services such as mortgages and student loans and expedite contractual agreements. And encrypted e-statements will be delivered directly to the bank customers' email in-box which will be protected by Arcot strong authentication so that only the intended customer will be able to view the statement. It will also enable the bank to launch sophisticated one-to-one marketing/coupon campaigns tailored to individual customers.

The bank's management team looks forward to leveraging the Arcot solution to enable a range of convenience and revenue-generating applications that will continue to improve their ROI.

About Arcot Systems

Arcot provides users with multi-factor, strong authentication with the simplicity of a password. Arcot makes online transactions safe for millions of customers by blocking fraud and protecting access. Its software-only solutions eliminate the need for expensive hardware and complex login processes. Arcot provides users with multi-factor, PKI-based authentication with the simplicity of a password.

For more information, please visit www.Arcot.com, email sales@arcot.com, or contact your nearest sales office:



Corporate Headquarters, U.S.

Arcot Systems, Inc.
Ph: +1 408 969 6100

United Kingdom

Arcot International
Ph: +44 118 965 7998

Germany

Arcot Deutschland GmbH
Ph: +49 8157 997793

India

Arcot R&D Software Private Ltd
Ph: +91 9886 238 131

www.arcot.com

Copyright © 2008 Arcot Systems, Inc. All rights reserved. Arcot, Arcot WebFort and ArcotID are registered trademarks of Arcot Systems, Inc. All other trademarks are the property of Arcot Systems, Inc. or their respective owners.